

普通高等教育“十一五”国家级规划教材

教育部“高等学校教学质量与教学改革工程”立项项目

孙建国 张国印 编著

网络安全实验教程

计算机科学与技术专业实践系列教材

清华大学出版社



教育部“高等学校教学质量与教学改革工程”立项项目
普通高等教育“十一五”国家级规划教材
计算机科学与技术专业实践系列教材

网络安全实验教程

孙建国　张国印　编著

清华大学出版社
北　京

内 容 简 介

本书基于网络安全体系结构，选择最新的网络安全实用软件和技术，在基本的网络安全实用技术和理论基础上，系统地讲授网络分析、远程控制技术、SSL VPN 技术、防火墙技术、入侵检测技术和虚拟蜜网技术等网络安全实验内容。本书不仅介绍网络安全体系结构基本理论和方法，还设计了多个应用工具实例。通过 Sniffer 分析软件、pcAnywhere 远程控制程序、Snort 入侵检测系统以及 Honeywall 蜜网架构等实验用例的训练，学生可以建立网络信息安全的体系概念，了解网络协议、数据包结构、网络安全管理技术等在计算机系统中的重要性。

本书取材新颖，采用实例教学的组织形式，内容由浅入深，循序渐进。书中给出了大量设计实例及扩展方案，不仅可以作为教学内容进行学习，而且部分内容还具有工程实践价值。本书可作为高等院校计算机类、电子类和自动化类等有关专业的教材和参考书。

图书在版编目（CIP）数据

网络安全实验教程/孙建国，张国印编著．—北京：清华大学出版社，2011.7
（计算机科学与技术专业实践系列教材）
ISBN 978-7-302-25530-7

Ⅰ．①网… Ⅱ．①孙… ②张… Ⅲ．①计算机网络－安全技术－高等学校－教材
Ⅳ．①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 087937 号

责任编辑：张瑞庆 王冰飞
责任校对：时翠兰
责任印制：李红英

出版发行：清华大学出版社　　**地　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　编**：100084
社 总 机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62795954，jsjjc@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　销：全国新华书店
开　本：185×260　　**印　张**：11.5　　**字　数**：262 千字
版　次：2011 年 7 月第 1 版　　**印　次**：2011 年 7 月第 1 次印刷
印　数：1～3000
定　价：19.50 元

产品编号：038583-01

普通高等教育"十一五"国家级规划教材
计算机科学与技术专业实践系列教材

编　委　会

前　　言

1. 写作背景

目前,关于我国高等教育的信息安全学科和专业方向设置问题受到非常大的关注。对于信息安全专业的本科生教育而言,其基本的培养方案、课程设置和教学大纲都需要根据新的形势进行变革,保密与信息安全专业方向也在积极的进行准备。

在新形势下,对于信息安全专业人才的培养标准是:具有宽厚的理工基础,掌握信息科学和管理科学专业基础知识,系统地掌握信息安全与保密专业知识,具有良好的学习能力、分析与解决问题能力、实践与创新能力。特别是在能力方面,要求信息安全专业的学生能够做到:具有设计和开发信息安全与防范系统的基本能力;具有获取信息和运用知识解决实际问题的能力;具有良好的专业实践能力和基本的科研能力。

实践学时的设置不仅起到加深学生理论课所学知识的作用,还起到培养学生建立理论与实践联系并解决实际问题的能力的作用,这对于实现当前的高等教育改革目标,提高毕业生综合素质具有重要的意义。但是受实验设备所限,各课程的实验环节较分散,分布在不同的实验平台或实验课程中,缺乏连贯性和整体性。网络安全实践环节的设立,是对计算机网络、现代密码学、信息系统安全、网络安全、软件安全、信息安全管理等专业核心课程的有效支撑。

本教材的编写思路是:从网络安全的体系架构中确定需要重点讲授和考核的内容,针对具体内容选择最具代表性的实用型软件工具或主流技术,开展具有基础实验和扩展实验相结合的实验内容,既满足于日常的实验教学活动,又能够促进学生创新实践能力的培养和提高。

2. 本书特点

本书兼顾高等学校理论教学需要与培养学生实践能力的需求,借鉴国外名校在信息安全专业课程设置及相关课程内容安排,组织本教程的相关理论知识及实验用例设计,力争理论详尽、用例科学、指导到位。配合高等学校的计算机网络、现代密码学、信息系统安全、网络安全、软件安全、信息安全管理等课程的实践教学环节,突出实用性,所有实验可操作性强,与实践结合紧密。本书不仅介绍网络安全的核心理论和主要技术,更着眼于介绍在网络安全管理和实践过程中如何运用系统软件,支撑和维护网络健康运行。

本书可作为信息安全专业及相关专业“计算机网络”、“现代密码学”、“信息系统安全”、“网络安全”、“信息安全管理”等课程的实践教材,书中的全部实验示例都经过精心的设计和完全的调试,可以放心使用。

3. 内容安排

本书的内容安排如下:

✍ 第 1 章介绍网络安全的基本概念和发展历程,以及网络安全与信息安全的密切联系,并介绍网络安全实验的特点和基本要求。

✍ 第 2 章介绍网络安全的研究意义和研究内容，主要包括密码学、防火墙技术、网络入侵检测、数据备份与容灾、防病毒技术，还介绍了网络管理规范。

✍ 第 3 章介绍网络分析实验的原理和技术，重点介绍基于 Sniffer Pro 嗅探软件的数据包捕获、网络监视等功能，并增加对多种网络协议进行嗅探分析的扩展实验环节。

✍ 第 4 章以 pcAnywhere 远程控制软件为主要工具，介绍其安装和使用方法，讲解主控端、被控端的配置方法，并介绍远程文件控制的操作方式。

✍ 第 5 章介绍 SSL VPN 概念，以及 VPN 服务配置与使用的操作方法。

✍ 第 6 章介绍防火墙技术，并结合天网防火墙和瑞星防火墙，讲述防火墙使用及配置方法。

✍ 第 7 章介绍入侵检测技术，重点讲述 Snort 入侵检测工具的使用方法。

✍ 第 8 章讨论对虚拟蜜网系统的实用性意义，介绍虚拟蜜网的搭建与攻击分析方法。

4. 致谢

首先感谢哈尔滨工程大学计算机科学与技术学院计算机实验教学中心的各位老师和研究生，感谢他们的大力支持和热情帮助。以下同学参与了本书实验示例代码的编写和调试以及原始资料的翻译和整理工作：王亚卓、陈明涛、李玲、董国忠、郝钟翁、周沫等，感谢他们付出的辛勤劳动。马春光老师担任了本教材的主审，感谢他的热情帮助。

感谢评阅专家对本书提出的宝贵修改意见，这些意见对于提高和完善全书质量起到了关键的作用。

编者虽然从事信息安全实践教学多年，但是由于水平所限，书中疏漏之处在所难免，诚恳地欢迎各位读者提出宝贵意见，编者的联系方式为：sunjianguo@hrbeu. edu. cn。

编　者

2011 年 1 月

目　　录

第 1 章　网络安全实验概述

1.1　引论

1.1.1　网络安全现状及发展

网络安全是指网络系统的软件、硬件及其存储的数据处于保护状态，网络系统不会由于偶然的或者恶意的冲击而受到破坏，网络系统能够连续可靠地运行。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、信息论等多研究领域的综合性学科。概括地说，凡是涉及网络系统的保密性、完整性、可用性和可控性的相关技术和理论都是网络安全的研究内容。

1.1.1.1　网络安全问题

随着计算机技术和互联网技术的飞速发展，数字化信息已经成为社会发展的重要资源。例如，数字化城市、数字化国防的建设都需要大量网络信息支持。快速发展的各类网络将这些数字信息紧密地联系在一起，与之相伴的是随时可能发生的各类安全问题，列举如下：

- 人为安全问题，如信息泄露、信息窃取、数据篡改、计算机病毒。
- 设备安全问题，如自然灾害、设计缺陷、电磁辐射。

2010 年 3 月，国家计算机网络应急处理协调中心发布了《2009 年中国网民网络信息安全状况调查报告》，报告对我国的网络安全现状进行了总体分析，突出表现概括为：

- 国内半数网民无法区分各类安全软件的异同。
- 2009 年，半数网民曾遭遇网络安全事件，网络下载和浏览成为病毒和木马传播的主要渠道。
- 网络安全问题对网民造成的损失主要是时间成本，其次才是经济方面的损失。
- 2009 年，网民处理安全事件所支出的服务费用共计 153 亿元人民币。
- 网络安全事件造成的虚拟财产损失成为网络安全事件的主要经济损失之一，虚拟财产保护亟待加强。
- 2009 年网络安全事件受关注度比以往大幅提升。
- 网民对网络的安全感降低，提供网上个人信息比以往更加慎重。
- 近 2100 万网民缺乏密码设置方面的保护意识。
- 99%的网民对于个人计算机均采取一定的防范措施。
- 近七成网民能够意识到个人网络安全问题会波及公共网络及他人的安全。

随着互联网的发展，各种安全问题层出不穷，互联网上蔓延和传播的恶意程序呈几何级数递增。国家计算机网络应急处理协调中心的调查结果显示，2009 年，52%的网民曾遭遇过网络安全事件。遭遇过网络安全事件的网民一般是通过很直观的方式来判断遭受

攻击的，通常是在使用计算机的过程中发现异常。71.9%的网民发现浏览器配置被修改，50.1%的网民发现网络系统无法使用，45%的网民发现数据、文件被损坏，41.5%的网民发现操作系统崩溃，而发现QQ密码、MSN密码、邮箱账号曾经被盗的网民占32.3%，如图1.1所示。

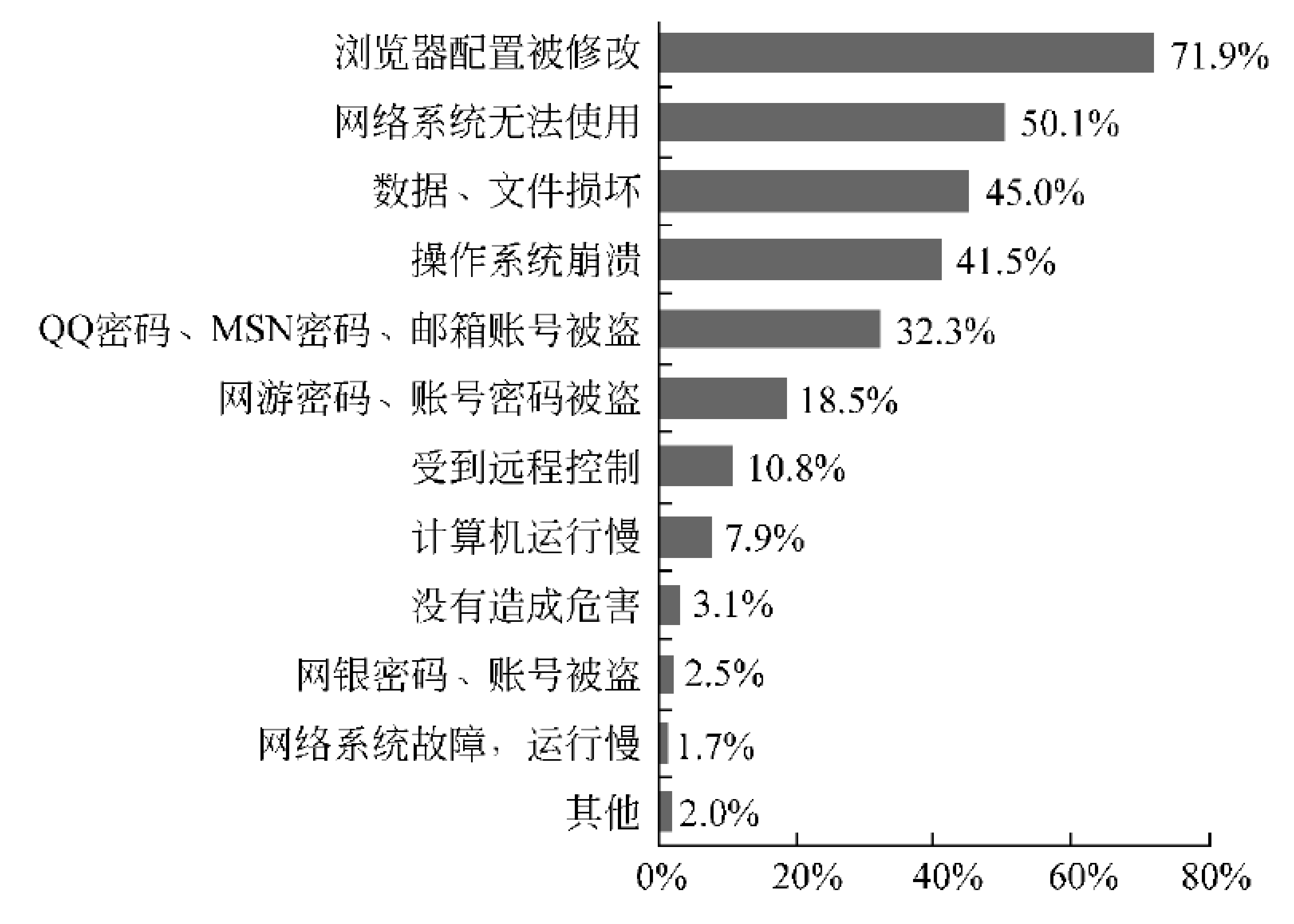


图 1.1　网络安全事件带来的危害

对网民用于处理网络安全事件支出的费用，国家计算机网络应急处理协调中心进行统计显示：2009年，网民处理安全事件所支出的服务费用共计153亿元人民币；在实际产生费用的人群中，人均费用约588.9元；费用在100元及以下的占51.2%；如按国内3.84亿网民计算，人均处理网络安全事故的费用约为39.9元，如图1.2所示。

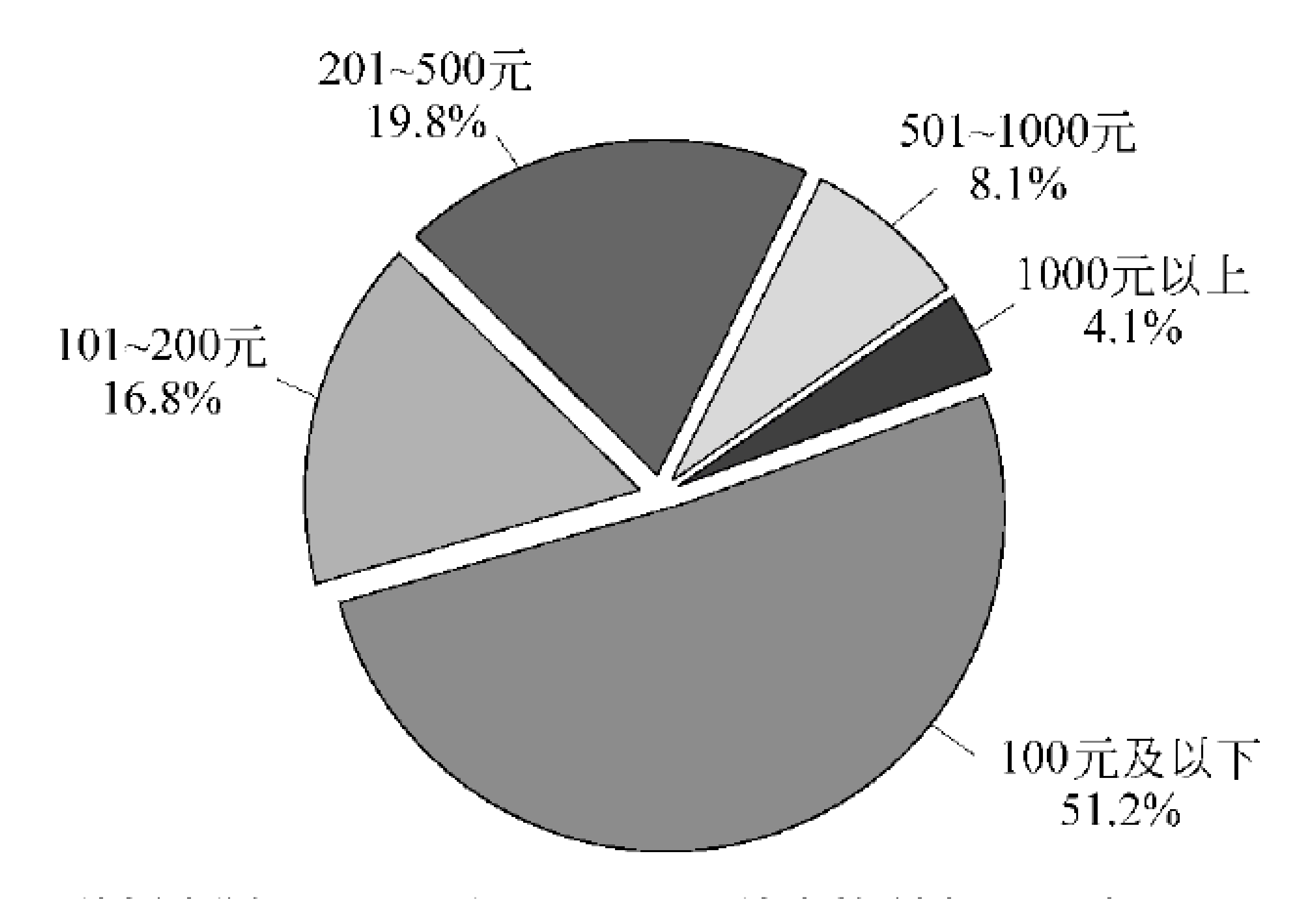


图 1.2　网络安全事件带来的直接经济损失情况

中国的网络安全技术在近几年得到快速的发展，这一方面得益于从中央到地方政府的广泛重视，另一方面因为网络安全问题日益突出，网络安全企业不断研发最新安全技

术,不断推出满足用户需求、具有时代特色的安全产品,促进了网络安全技术的发展。

1.1.1.2 网络安全技术

网络安全技术主要包括防火墙技术、入侵检测技术以及防病毒技术。这三种网络安全技术是针对数据、单一系统以及软硬件本身的安全保障,具体原因包括三个方面:

首先,从用户角度来看,虽然安装了防火墙,但是仍避免不了蠕虫、垃圾邮件、病毒以及拒绝服务攻击等网络危害事件的发生。

其次,入侵检测产品在提前预警方面存在不足,对于危害程序和代码的精确定位以及系统全局管理能力还有很大的提升空间。

最后,虽然很多用户在系统终端上都安装了防病毒产品,但是内网安全问题仍然突出,尤其是安全策略的执行、外来非法侵入、补丁管理以及操作行为规定等方面。

目前来看,网络安全的防护重点将集中在信息语义范畴和网络行为。

1.1.1.3 网络安全发展趋势

在网络混合攻击时代,功能单一的防火墙系统无法满足业务的需要,防火墙技术必须具备多种安全功能,如基于应用协议层防御,低误报率检测,高可靠性、高性能的平台和统一组件化管理技术等,由此,UTM(unified threat management,统一威胁管理)技术应运而生。

UTM 在统一的产品管理平台下,集防火墙、VPN、网关防病毒、IPS、拒绝服务攻击等众多产品功能于一体,实现了多种防御功能。向 UTM 方向演进将是防火墙的发展趋势。

UTM 设备应具有以下特点:

(1) 网络安全协议层防御。UTM 设备主要针对 IP 地址、端口等静态信息进行防护和控制,除了传统的访问控制外,还需对垃圾邮件、拒绝服务、黑客攻击等外部威胁进行综合检测和主动防御。

(2) 通过分类检测技术降低误报率。串联接入的网关设备一旦误报过高,将会严重影响系统的正常服务,给用户带来灾难性的后果。IPS 理念在 20 世纪 90 年代就被提出,但是目前 IPS 部署非常有限,影响其部署的一个重要问题就是误报率过高。分类检测技术可以大幅度降低误报率,针对不同的攻击类型,采取不同的检测技术,比如防御拒绝服务攻击、防蠕虫和黑客攻击、防垃圾邮件攻击等,从而显著降低误报率。

(3) 高可靠性、高性能的硬件支撑平台。

(4) 一体化管理。UTM 设备具有能够统一控制和管理的平台,使用户能够有效地管理。设备平台可以实现标准化并具有可扩展性,用户可在统一的平台上进行组件管理,同时,一体化管理也能消除信息产品之间由于无法沟通而带来的信息孤岛,从而在应对各种各样攻击威胁的时候,更好地保障用户的网络安全。

1.1.1.4 网络威胁趋势分析

在信息网络普及的时代,信息安全威胁随时存在,且不断增加,信息网络安全性正逐步得到人们的重视。在当前复杂的网络应用环境下,信息网络所面临的安全形势异常严峻。来自中国电子商务研究中心的报告列举了如下严重的网络威胁。

1. 垃圾邮件和网络欺骗

社交网站成为网络安全的重灾区。2010年，Koobface蠕虫等安全问题对社交网站用户形成巨大威胁。从这些软件攻击过程来看，正逐步由攻击系统、窃取资料的被动方式转变为主动攻击模式。安全专家认为，恶意软件作者正在拓展攻击范围，把恶意软件植入社交网站应用层内部，攻击者可以毫无限制地窃取用户的资料和登录密码。

思科在其2009年《年度安全报告》中揭示了社交媒体(尤其是社交网络)对网络安全的影响，并探讨了个体本身在为网络犯罪创造机会方面所起的关键作用。社交网络已经成为网络犯罪的导火索，网站成员过于信任社区伙伴，根本没有采取任何阻止恶意软件和计算机病毒的预防措施。这些不良用户行为以及系统、操作漏洞结合在一起会具有不可估量的破坏性，将大幅增加网络安全风险。

2. 云计算为网络犯罪提供了新的技术

云计算在2009年取得了重大的发展，但应该清醒地认识到：市场的快速发展会牺牲一定的安全性，攻击者今后将把更多的时间用于挖掘云计算服务提供商的API(应用编程接口)漏洞方面。

随着越来越多的IT功能通过云计算来提供，网络犯罪也顺应了这一趋势。网络攻击者和黑客也将效仿企业做法使用基于云计算的工具，以便更有效率地部署远程攻击，甚至借此大幅拓展攻击范围。

对于云计算将被黑客所利用这个严峻的问题，各大安全公司都把精力放在与云计算相关的安全服务上，提供加密、目录管理、反垃圾邮件、恶意程序扫描等各类解决方案。据悉，著名安全评测机构VB100号召安全行业联合起来，组成一个对抗恶意程序的共同体，分享技术和资源。

3. 智能手机安全问题愈发严重

随着移动通信业务应用的不断增多，智能设备的受攻击范围也在不断扩大，移动通信安全所面临的问题将会越来越严重。目前，已经出现了手机蠕虫病毒、智能手机盗号木马，虽然这些病毒还不能自我传播，还需要依靠计算机来传播，但是可以预计到，具有自我传播能力的病毒势必出现，将严重威胁各类移动通信终端设备。

总体而言，安全专家认为，随着智能手机业务范围的拓广，用户利用手机来处理银行交易、社交网站和其他业务，黑客将越来越关注这一攻击领域。

4. 搜索引擎成为黑客的全新赢利方式

黑客不断寻找新的方法借助钓鱼网站吸引用户，利用搜索引擎优化技术展开攻击便是其中的一种方法。谷歌和必应(Bing)对实时搜索的支持也将吸引黑客进一步提升相关技术。作为一种攻击渠道，搜索引擎是非常理想的选择，因为用户通常都非常信任搜索引擎，对于排在前几位的搜索结果更是没有任何怀疑，这就给了黑客可乘之机，黑客可以利用搜索引擎对用户发动攻击。

5. “僵尸网络”继续猖獗

所谓僵尸，是指受恶意软件感染而被犯罪分子远程操控的个人计算机。犯罪分子通过网络将病毒植入成千上万台个人计算机，实现大范围的操控，犯罪分子们使用这些计算机进行各种网络犯罪，如垃圾邮件发送、服务阻断攻击、网络钓鱼及非法主机攻击等，基本

覆盖了所有网络犯罪行为。从当前的网络安全态势来看，越来越多的计算机受到感染，而被感染的时间也越来越长了。

6. 传统攻击方式再度兴起

IBM X-Force团队预计，大规模蠕虫攻击将再度兴起，与此同时，DDoS（分布式拒绝服务攻击）也将重新成为主流攻击方式，木马仍将占据主要地位。

来自中国电子商务研究中心的报告显示，据Websense的卢纳德预计，电子邮件攻击也有重新抬头之势。研究人员已经发现，通过PDF等邮件附件发动的攻击开始增加。他说："恶意邮件攻击在2005年至2008年期间已经销声匿迹。而现在不知出于何种原因，这种攻击方式又再度出现。"

从网络威胁方式来看，威胁方式的演进主要体现在如下几个方面。

1）实施网络攻击的主体发生了变化

实施网络攻击的主要人群正由好奇心重、炫耀攻防能力的兴趣型黑客群，向更具犯罪思想的赢利型攻击人群过渡，针对终端系统漏洞实施"zero-day攻击"和利用网络攻击获取经济利益，逐步成为主要趋势。其中以僵尸网络、间谍软件为手段的恶意代码攻击，以敲诈勒索为目的的分布式拒绝服务攻击，以网络仿冒、网址嫁接、网络劫持等方式进行的在线身份窃取等安全事件持续快增，而针对P2P、IM等新型网络应用的安全攻击也在迅速发展。以"熊猫烧香"、"灰鸽子"事件为代表形成的黑色产业链，也凸显了解决信息安全问题的迫切性和重要性。

2）企业对安全威胁的认识发生了变化

过去，企业信息网络安全的防护中心一直定位于网络边界及核心数据区，通过部署各种各样的安全设备实现安全保障。但随着企业信息边界安全体系的基本完善，信息安全事件仍然层出不穷。对企业内部人员缺乏安全管理、办公时间肆意上网、计算机使用不当等都使网络信息安全风险变得更为严重。

3）安全攻击的主要手段发生了变化

安全攻击的手段多种多样，典型的手段包含拒绝服务攻击、非法接入、IP欺骗、网络嗅探、木马攻击以及垃圾邮件等方式。随着攻击技术的发展，攻击手段正由单一攻击模式向多种攻击手段结合的复合性攻击发展。结合多种攻击手段的复合模式所带来的危害，远远大于单一模式的攻击，且更加难以控制。

1.1.2 黑客及黑客入侵技术

1.1.2.1 黑客定义

黑客是计算机应用领域中的一个特殊的群体，随着计算机系统被攻击报道的逐渐增多，黑客越发成为业界的关注焦点。黑客是英文hacker一词的音译，是指计算机系统的非法入侵者。

在早期麻省理工学院的校园俚语中，"黑客"有"恶作剧"之意，尤指手法巧妙、技术高明的恶作剧；在日本《新黑客词典》中，对黑客的定义是"喜欢探索软件程序奥秘，并从中增长了个人才干的人"。目前，黑客被准确界定为"以保护网络为目的，具有软硬件高级知识，有能力通过创新的方法剖析系统的技术精英，他们以侵入为手段找出网络漏洞，进而

令互联网络趋于完善和安全”。一般认为,黑客起源于20世纪50年代麻省理工学院的实验室中,他们热衷于解决难题。

20世纪60、70年代,“黑客”富于褒义,专指那些独立思考、奉公守法的计算机爱好者,这些人智力超群,对计算机技术全身心投入,在他们看来,黑客活动意味着对计算机的最大潜力进行智力上的自由探索,为计算机技术的发展做出巨大贡献。正是这些黑客,倡导了一场个人计算机革命,倡导了现行的计算机开放式体系结构。现在黑客使用的入侵计算机系统的基本技巧,如破解口令(password cracking)、开天窗(trapdoor)、走后门(backdoor)、安放特洛伊木马(Trojan horse)等,都是在这一时期发明的。从事黑客活动的经历,成为后来许多计算机业巨子简历上不可或缺的一部分。例如,苹果公司创始人之一乔布斯就是一个典型的例子。

到了20世纪80、90年代,计算机越来越重要,大型数据库也越来越多,信息越来越集中在少数人的手里。黑客认为,信息应共享而不应被少数人所垄断,于是将注意力转移到涉及各种机密的信息数据库上。而这时,计算机化空间已私有化,成为个人拥有的财产,社会不能再对黑客行为放任不管,而必须采取行动,利用法律等手段来进行控制,黑客活动受到了打击。目前,许多政府机构已经邀请黑客为他们检验系统的安全性,甚至还请他们设计新的安保规程。

与黑客相对的是骇客,骇客是cracker的音译,就是“破坏者”的意思。骇客是贬义的,骇客具备广泛的计算机知识,他们做的事情更多的是破解商业软件,恶意入侵别人的网站并造成损失,利用网络漏洞破坏网络。

黑客和骇客的基本差异在于,黑客是有建设性的,而骇客则专门搞破坏。对于一个黑客来说,学会入侵和破解是必要的,但最主要的还是编程。对于一个骇客来说,他们只追求入侵的快感,不在乎技术,他们不会编程,不知道入侵的具体细节。还有一种情况是试图破解某系统或网络以提醒该系统所有者的系统安全漏洞,这群人往往被称做“白帽黑客”或“匿名客”(sneaker)或红客。许多这样的人是计算机安全公司的雇员,并在完全合法的情况下攻击某系统。

1.1.2.2 黑客活动

黑客的主要活动内容包括:

(1) 作为一个黑客,在找到系统漏洞并侵入的时候,往往都会很小心地避免造成麻烦,并且善意地提醒系统管理员,但是在这一过程中有许多因素都是未知的,没有人能断定最终会是什么结果,因此一个好的黑客是不会随便攻击个人用户及站点的。

(2) 编写一些有用的开源软件,这些软件都是免费的、公开的。

(3) 帮助别的黑客测试和调试软件。

(4) 黑客们都以探索漏洞与编写程序为乐,在黑客的圈子里,有许多其他事情可做,如维护和管理相关的黑客论坛、新闻组以及邮件列表,维持大的软件供应站点,推动RFC和其他技术标准等。

(5) 真正的黑客不会随意破解商业软件并将其广泛流传,也不会恶意侵入别人的网站并造成损失,黑客的所作所为应当更像是对于网络安全的监督。

1.1.2.3 黑客事件

历史上,发生过许多著名的黑客入侵事件:

1979 年,年仅 15 岁的凯文·米特尼克仅凭一台计算机和一部调制解调器闯入了北美空中防务指挥部的计算机主机。

1987 年,美联邦执法部门指控 16 岁的赫尔伯特·齐恩闯入美国电话电报公司的内部网络和中心交换系统。齐恩是美国 1986 年“计算机欺诈与滥用法案”生效后被判有罪的第一人。

1988 年,年仅 23 岁的大学生 Robert Morris 在 Internet 上释放了世界上首个“蠕虫”程序。Robert Morris 最初是把这个 99 行的程序放在互联网上进行试验,可结果却使得他的计算机被感染并迅速在互联网上蔓延开。Robert Morris 也因此在 1990 年被判入狱。

1990 年,为了获得在洛杉矶地区 kiis-fm 电台第 102 个呼入者的奖励——保时捷跑车,Kevin Poulsen 控制了整个地区的电话系统,以确保他是第 102 个呼入者。最终,他如愿以偿获得跑车并为此入狱三年。

1995 年,来自俄罗斯的黑客 Vladimir Levin 成为历史上第一个通过入侵银行计算机系统来获利的黑客,他侵入美国花旗银行并盗走 1000 万美金。

1996 年,美国黑客 Timothy Lloyd 曾将一个六行的恶意软件放在了其雇主 Omega 工程公司(美国航天航空局和美国海军最大的供货商)的网络上,此事件导致 Omega 公司损失 1000 万美金。

1999 年,年仅 30 岁的 David Smith 编写了 Melissa 病毒。它是世界上首个具有全球破坏力的病毒,它使世界上 300 多家公司的计算机系统崩溃。整个病毒造成的损失接近 4 亿美金。David Smith 随后被判处 5 年徒刑。

2000 年,年仅 15 岁的 MafiaBoy(由于年龄太小,因此没有公布其真实身份)在情人节期间成功侵入包括 eBay、Amazon 和 Yahoo 在内的大型网站服务器,并成功阻止了服务器向用户提供服务。他于 2000 年被捕。

2002 年 11 月,伦敦人 Gary McKinnon 在英国被指控非法侵入美国军方 90 多个计算机系统。

1994 年 4 月 20 日,中国 NCFC 工程通过美国 Sprint 公司连入 Internet 的 64kbps 国际专线开通,实现了与 Internet 的全功能连接,中国成为直接接入 Internet 的国家。从此,中国黑客开始了原始萌动。同年,中国第一部信息安全法规《中华人民共和国计算机信息系统安全保护条例》颁布实施。1997 年,《中华人民共和国计算机信息网络国际联网管理暂行规定》颁布实施。

1998 年 6 月 16 日,上海某信息网的工作人员在例行检查时,发现网络遭到不速之客的袭击。7 月 13 日,犯罪嫌疑人杨某被逮捕。这是我国第一例计算机黑客事件。

1999 年,中国黑客发展的历史上产生了一个高峰。这一年正是网络泡沫高度泛滥的顶峰,黑客在这一阵势不可挡的浪潮中不可避免地泛起了泡沫。从 1999 年到 2000 年,中国黑客联盟、中国鹰派、中国红客联盟等一大批黑客网站兴起,带来了黑客普及教育。

1.1.2.4 黑客入侵技术

黑客入侵一般分为信息收集、探测分析系统安全弱点以及实施攻击三个步骤。

信息收集是为了了解所要攻击目标的详细信息，通常黑客会利用相关的网络协议或实用程序来收集，常用的工具主要包括以下几种。

- SNMP 协议：用来查阅网络系统路由器的路由表，从而了解目标主机所在网络的拓扑结构及其内部细节。
- TraceRoute 程序：用来获得到达目标主机所要经过的网络数和路由器数。
- Whois 协议：该协议的服务信息能提供所有有关的 DNS 域和相关的管理参数。
- DNS 服务器：用来提供系统中可访问的主机的 IP 地址表和它们所对应的主机名。
- Finger 协议：用来获取一个指定主机上的所有用户的详细信息。
- Ping 实用程序：用来确定一个指定的主机的位置。

首先，当收集到目标相关信息以后，黑客会利用探测分析系统寻找系统的安全漏洞或设计缺陷。黑客发现“补丁”程序的接口后会自己编写程序，通过该接口进入目标系统。黑客还会使用 Telnet、FTP 等软件向目标主机申请服务，如果目标主机有应答就说明其开放了这些端口的服务。其次，黑客使用一些公开的工具软件，如 Internet 安全扫描程序(Internet security scanner，ISS)、网络安全分析工具 SATAN 等来对网络进行扫描，确定安全漏洞或使用特洛伊木马来获取攻击目标系统的非法访问权。

在获得目标系统的非法访问权限后，黑客会实施攻击，攻击可分为以下两种。

- 被动攻击：攻击者只观察和分析某一个协议数据单元(PDU)而不干扰信息流。例如，监听截获操作等。
- 主动攻击：攻击者对某个连接中通过的数据包进行各种处理。例如，更改报文流、拒绝报文服务、伪造连接初始化等。

攻击程度包括以下等级：

- 只获得访问权(登录名和口令)。
- 获得访问权，并毁坏、侵蚀或改变数据。
- 获得访问权，并获得部分系统或整个系统控制权，拒绝拥有特权用户的访问。
- 未获得访问权，通过攻击程序引起网络持久性或暂时性的运行失败、重新启动、挂起或其他无法操作的状态。

1. 黑客攻击过程

黑客攻击过程包括以下步骤：

(1) 隐藏自己的踪迹。通过清除日志、删除拷贝文件、进程隐藏、连接隐藏、使日志紊乱等方法销毁入侵痕迹，并在受攻击目标系统中为自己建立新的后门，以便继续访问该系统。

(2) 在目标系统内安装探测软件，如特洛伊木马或其他一些远程控制程序，继续收集感兴趣的信息和敏感数据。黑客还可以以目标系统为跳板向其他系统发起攻击。

(3) 在被攻击目标系统上进一步获得特许访问权，开展对整个系统的攻击，毁坏重要数据乃至破坏整个网络系统。

2. 主要入侵方式

1）密码破解

- 字典攻击：一种被动攻击，黑客获取系统的口令，然后利用字典进行匹配比较。字典攻击成功率较高。
- 伪造登录程序：通过伪造登录界面来获得用户输入的账号和密码。
- 密码探测程序：反复模拟 NT 的编码过程，并与 Windows NT 系统的 SAM 密码数据库内的数据进行匹配。
- 口令攻击：通过网络监听非法得到用户口令，然后利用软件强行破解用户口令；获得用户口令文件后暴力破解用户口令。
- 口令陷阱：在网络服务中设置虚假界面，要求用户输入用户名与口令，从而截获该用户的用户名与口令。
- 网络踩点：利用工具获取目标的一些有用信息，如域名、IP 地址、网络拓扑结构及相关用户信息。
- 协议栈指纹：利用探测包，从得到的响应中确定目标主机使用的操作系统。
- 会话劫持：在合法的通信连接建立后，可通过阻塞或摧毁通信的一方来接管已经建立起来的连接，从而假冒被接管方与对方通信。
- 非授权访问尝试：对被保护文件进行读、写或执行的尝试，也包括为获得被保护访问权限所做的尝试。

2）网络监听

网络监听又称为 IP 嗅探，是主机的一种工作模式。在这种模式下，主机可以接收到本网段在同一条物理通道上传输的所有信息。高级的窃听程序具有生成假数据包、解码等功能，甚至可锁定服务器的特定端口，自动处理与这些端口有关的数据包。利用上述功能，可监听他人的联网操作，窃取信息。

当信息以明文的形式在网络上传输时，便可以使用网络监听的方式进行攻击。将网络接口设置在监听模式便可以源源不断地将网上的信息截获。网络监听可以获取网络中所有的数据包。

3）系统漏洞与欺骗

- 漏洞是指系统本身的设计、操作和实现上的错误，这些漏洞在补丁未被开发出来之前一般很难防御黑客的破坏。
- 欺骗式主动式攻击，利用网络上的某台计算机来伪装另一台目标主机，以此欺骗网络中的其他计算机向伪造计算机发送数据或赋予权限。常见的欺骗方式包括 IP 欺骗、路由欺骗、ARP 欺骗以及 Web 欺骗。

4）端口扫描与特洛伊木马

在连续的非授权访问过程中，攻击者为了获得网络内部的信息，通常使用这种攻击尝试，典型示例包括 SATAN 扫描、端口扫描和 IP 半途扫描等。

黑客可以利用一些端口扫描软件，如 SATAN、IP Hacker 等对被攻击目标进行端口扫描，查看是否存在开放端口并进行通信操作。扫描器是自动监测远程或本地主机安全性弱点的程序。通过使用扫描器可以不留痕迹地发现远程服务器的各种 TCP 端口的分

配、提供的服务和软件版本，从而了解到远程主机所存在的安全问题。

特洛伊木马是一种基于远程控制的黑客工具。木马程序寄生在普通程序内部暗中进行某些破坏性操作或进行数据窃取，以完成某些特殊任务。

不能自我复制是特洛伊木马与病毒的最显著的区别。特洛伊木马原则上只是一种远程管理工具，而且本身不带伤害性，也没有感染力，所以不能称之为病毒，但却常常被视为病毒。目前的杀毒软件对木马有一定的预防和清除作用。

5）拒绝服务（denial of service，DoS）攻击

最基本的拒绝服务攻击方式就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务。目前已知的拒绝服务攻击就有几百种，它是最基本的入侵攻击手段，也是最难对付的入侵攻击手段之一。DoS 攻击分为四种：

- 利用 TCP/IP 协议中的 Bug 进行攻击，如 Ping of Death 和 Teardrop。
- 利用 TCP/IP 协议的脆弱性进行攻击，如 SYN Flood 和 Land 攻击。
- 用大量无用数据淹没一个网络，如 Smurf 攻击和 Fraggle 攻击。
- 分布式拒绝服务攻击（DDoS）。

6）WWW 欺骗技术

将用户浏览网页的 URL 指向黑客设定的服务器，当用户浏览目标网页的时候，实际上是向黑客服务器发出请求，达到欺骗的目的。

7）电子邮件攻击

电子邮件攻击主要表现为两种方式。

- 电子邮件轰炸：向同一信箱发送数以千计、万计甚至无穷多次的内容相同的垃圾邮件，致使电子邮件服务器操作系统瘫痪。
- 电子邮件欺骗：在正常的附件中加载病毒或其他木马程序。

8）缓冲区溢出

缓冲区溢出是一种系统攻击手段，通过向程序的缓冲区写入超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他指令，以达到攻击的目的。据统计，通过缓冲区溢出进行的攻击占所有系统攻击总数的 80%以上。一般情况下，覆盖其他数据区的数据是没有意义的，最多造成应用程序错误。但是，如果输入的数据是经过精心设计的，覆盖缓冲区的数据恰恰是入侵程序代码，入侵者就获取了程序的控制权。

此外，入侵方式还包括社会工程学攻击、黑客软件攻击以及跳板攻击等。

3. 主要防范措施

可采取的防范黑客入侵的措施主要包括数据加密、身份认证、完善访问控制策略、审计等。

- 身份认证是指通过密码或特征信息来确认用户身份的真实性，对重要主机单独设立一个网段，以避免机器被攻破后造成整个网段通信全部暴露。
- 完善访问控制策略，设置访问权限、目录安全等级控制、防火墙安全控制等，研究清楚各进程必需的进程端口号，关闭不必要的端口。
- 审计是指把系统中和安全相关的事件全部记录下来，对用户开放的各个主机的日志文件全部定向并集中管理，定期检查备份日志主机上的数据、系统日志文件和

关键配置文件。

- 下载安装最新的操作系统及其他应用软件的安全和升级补丁，安装几种必要的安全加强工具，对系统进行完整性检查。
- 制定详尽的入侵应急措施以及汇报制度。发现入侵迹象，立即打开进程记录功能，同时保存内存中的进程列表以及网络连接状态，保护当前的重要日志文件。

1.1.2.5 入侵检测技术

入侵检测技术的核心问题是截获有效的网络信息。目前主要是通过两种途径来获取信息：

- 通过网络侦听程序（如 Sniffer、Vpacket 等）来获取网络信息（数据包信息、网络流量信息、网络状态信息、网络管理信息等）。
- 通过对操作系统和应用程序的系统日志进行分析，来发现入侵行为和系统潜在的安全漏洞。

入侵检测的基本手段是采用模式匹配的方法来发现入侵攻击行为，典型的入侵检测方式包括以下内容：

1）Land 攻击

Land 攻击是一种拒绝服务攻击。由于 Land 攻击的数据包中的源地址和目标地址是相同的，因此当操作系统接收到这类数据包时，不知道该如何处理堆栈中通信源地址和目的地址相同的这种情况，或者循环发送和接收该数据包，消耗大量的系统资源，从而造成系统崩溃或死机。

检测方法：判断网络数据包的源地址和目标地址是否相同。配置防火墙或过滤路由器的过滤规则，并对这种攻击进行审计，记录事件发生的时间、源主机和目标主机的 MAC 地址和 IP 地址。

2）TCP SYN 攻击

TCP SYN 攻击是一种拒绝服务攻击。利用 TCP 客户机与服务器之间三次握手过程的缺陷来进行。攻击者通过伪造源 IP 地址向被攻击者发送大量的 SYN 数据包，当被攻击主机接收到大量的 SYN 数据包时，需要使用大量的缓存来处理这些连接，并将 SYN ACK 数据包发送回错误的 IP 地址，并一直等待 ACK 数据包的回应，最终导致缓存用完，不能再处理其他合法的 SYN 连接，对外提供正常服务。

检测方法：检查单位时间内收到的 SYN 连接是否超过系统设定的值。当接收到大量的 SYN 数据包时，通知防火墙阻断连接请求或丢弃这些数据包，并进行系统审计。

3）Ping Of Death 攻击

Ping Of Death 攻击是一种拒绝服务攻击。由于部分操作系统接收到长度大于 65535 字节的数据包时，会造成内存溢出、系统崩溃等后果，从而达到攻击的目的。

检测方法：判断数据包的大小是否大于 65535 个字节。使用补丁程序，当收到大于 65535 个字节的数据包时，丢弃该数据包，并进行系统审计。

4）WinNuke 攻击

WinNuke 攻击是一种拒绝服务攻击。特征是攻击目标端口，被攻击的目标端口通常是 139、138、137、113、53，而且 URG 位设为“1”，即紧急模式。

检测方法：判断数据包目标端口是否为139、138、137等，并判断URG位是否为“1”。配置防火墙设备或过滤路由器，并对这种攻击进行审计。

5）Teardrop攻击

Teardrop攻击是一种拒绝服务攻击。其工作原理是向被攻击者发送多个分片的IP包，某些操作系统收到含有重叠偏移的伪造分片数据包时将会出现系统崩溃、重启等现象。

检测方法：对接收到的分片数据包进行分析，计算数据包的片偏移量(Offset)是否有误。添加系统补丁程序，丢弃收到的病态分片数据包，并对这种攻击进行审计。

6）TCP/UDP端口扫描

TCP/UDP端口扫描是一种预探测攻击。对被攻击主机的不同端口发送TCP或UDP连接请求，探测被攻击对象运行的服务类型。

检测方法：统计外界对系统端口的连接请求，特别是对21、23、25、53、80、8000、8080等以外的非常用端口的连接请求。当收到多个TCP/UDP数据包对异常端口的连接请求时，通知防火墙阻断连接请求，并对攻击者的IP地址和MAC地址进行审计。

1.1.2.6 计算机取证

计算机取证又称为数字取证或电子取证，是指对计算机入侵、破坏、欺诈、攻击等犯罪行为利用计算机软硬件技术，按照符合法律规范的方式进行证据获取、保存、分析和出示的过程。从技术上看，计算机取证是一个对受侵计算机系统进行扫描和破解，以及对整个入侵事件进行重建的过程。计算机取证包括以下两个阶段。

- 物理证据获取：指调查人员到计算机犯罪或入侵现场，寻找并扣留相关的计算机硬件。
- 信息发现：指从原始数据中寻找可以用来证明或者反驳的证据，即电子证据。

物理取证是核心任务。物理证据的获取是全部取证工作的基础。获取物理证据，保证原始数据不受任何破坏，应遵守如下操作规定：

- 不改变原始记录。
- 不在作为证据的计算机上执行无关的操作。
- 不给犯罪者销毁证据的机会。
- 详细记录所有的取证活动。
- 妥善保存得到的物证。

如果被入侵的计算机处于工作状态，取证人员应该设法保存尽可能多的犯罪信息。

物理取证不但是基础，而且是技术难点。案件发生后，应立即对目标机和网络设备进行内存检查并做好记录，根据所用操作系统的不同可以使用内存检查命令对内存里易删除数据进行保存，力求不要对硬盘进行任何读写操作，以免更改数据原始性。利用专门的工具对硬盘进行逐扇区的读取，将硬盘数据完整地复制出来，便于对原始硬盘的镜像文件进行分析。

在道德感化、技术防范的同时，无疑也离不开法律手段的辅助作用，需要依靠一定刑罚威慑力的保障。美国是世界上最早发明计算机的国家，也是世界上最早对计算机黑客

行为进行立法规范的国家。从某种意义上讲,美国反计算机犯罪的立法,对其他国家开展相关工作提供了许多可资借鉴的经验和教训。其中,最著名的有《1984 年计算机欺诈和滥用法》。

在我国,1994 年国务院颁布的《计算机信息系统安全保护条例》,是第一个对计算机信息系统安全进行保护的条例。该条例没有规定计算机犯罪的罪名,但是第 24 条规定,对于违反本条例的规定构成犯罪的,依法追究刑事责任。此后,1996 年国务院发布《计算机信息网络国际联网管理暂行规定》(1997 年作了修正);1997 年公安部发布《计算机信息网络国际联网安全保护管理办法》;1998 年,国务院信息化工作领导小组发布《计算机信息网络国际联网管理暂行规定实施办法》;国家保密局发布《计算机信息系统保密管理暂行规定》;公安部、中国人民银行发布《金融机构计算机信息系统安全保护工作暂行规定》。这一系列法律法规和相关规定共同构成了一个计算机信息系统和网络安全保护的初步法律框架。

随着计算机安全与犯罪问题日益严重,公安部授权起草了涉及计算机安全与犯罪问题的专门性法条,在 1997 年刑法修订中,增加了关于计算机安全与犯罪的三个条款,即第 285 条、第 286 条和第 287 条。1997 年 12 月 9 日最高人民法院审判委员会第 951 次会议通过的《关于执行〈中华人民共和国刑法〉确定罪名的规定》,规定了两个罪名,即非法侵入计算机信息系统罪和破坏计算机信息系统罪。2000 年 12 月 28 日,九届全国人大常委会第十九次会议表决通过《全国人民代表大会常务委员会关于维护互联网安全的决定》,规定对于侵入国家事务、国防事务、尖端科学技术领域的计算机信息系统的行为构成犯罪的,依照刑法有关规定追究刑事责任。这进一步强化了我国打击计算机黑客行为的法律体系。

1.1.3 网络安全主要影响因素

网络安全的主要影响因素包括以下几个方面:

1)系统安全漏洞

常用的各种操作系统几乎都或多或少存在安全漏洞。系统漏洞分为两种:有意漏洞和无意漏洞。有意漏洞是软件代码编写者有意设置的,目的在于当失去对系统的访问权时,仍能进入系统。无意漏洞是指在编写软件代码时无意留下的缺陷或不足。

据统计,目前发现的系统安全漏洞的数量已经接近病毒的数量。典型安全漏洞如远程获得超级用户 root 权限、远程过程调用(RPC)服务以及它所安排的无口令入口。

目前流行的许多操作系统均存在网络安全漏洞,如 UNIX 和 Windows。黑客往往就是利用这些操作系统本身所存在的安全漏洞侵入系统,具体包括以下几个方面:(1)稳定性和可扩充性方面。由于设计的系统不规范、不合理以及缺乏安全性考虑,因而使其受到影响。网络应用的需求没有引起足够的重视,设计和选型考虑欠周密,从而使网络功能发挥受阻,影响网络的可靠性、扩充性和升级换代。(2)网卡工作站选配不当,导致网络不稳定,缺乏安全策略。许多站点在防火墙配置上无意识地扩大了访问权限,忽视了这些权限可能会被其他人员滥用;此外,访问控制配置的复杂性容易导致配置错误,从而给他人以可乘之机。

2）TCP/IP 协议安全

TCP/IP 协议原理公开，存在很大的安全隐患，缺乏强健的安全机制。当安全工具发现并努力更正某方面的安全问题时，其他的安全问题又出现了。因此，黑客总是可以使用先进的手段进行攻击。

3）物理安全问题

完整准确的安全评估是黑客入侵防范体系的基础。它可以对现有或将要构建的网络安全防护性能作出科学、准确的分析评估。网络安全评估分析就是对网络进行检查，确定是否存在可能被黑客利用的漏洞，并对发现的问题提出建议，从而提高网络系统安全性能。

4）人为因素

人为因素包括人为的无意失误、恶意攻击及管理缺失，来自内部用户的安全威胁远大于外网用户的安全威胁。使用者缺乏安全意识，许多应用服务系统在访问控制及安全通信方面考虑较少，如果系统设置错误，很容易造成损失。

1.2 网络安全基本知识

互联网为人们提供了快速、便捷的通信手段，促进了计算机网络技术在社会、经济各领域的广泛应用，同时也为伺机窃取利益信息的不法之徒提供了犯罪场地。随着计算机网络应用范围的不断扩大，网络安全问题已成为当今社会的一个焦点。据伦敦英国银行协会统计，全球每年因计算机犯罪造成的损失大约为 80 亿美元。而计算机安全专家则指出，实际损失金额应在 100 亿美元以上。

1.2.1 网络安全研究内容

网络安全包括以下三个方面的内容：

（1）计算机实体的安全。在一定的环境下，对网络系统中设备的安全保护。

（2）网络系统运行安全。在实体安全前提下，保证网络系统不受偶然的或恶意的威胁，能够连续可靠地运行，正常的网络服务不中断。

（3）信息安全。在网络内存储和处理的信息资源具有绝对的保密性、完整性和可用性，不存在被泄露、更改和破坏的风险。网络系统的信息安全目标包括以下几点。

- 保密性（confidentiality）：防止信息的非授权访问或泄露。信息只限于授权用户使用，保密性主要通过信息加密、身份认证、访问控制、安全通信协议等技术实现，信息加密是防止信息非法泄露的最基本手段。
- 完整性（integrity）：保证信息不会被非法改动和销毁。保密性强调信息不能非法泄露，而完整性强调信息在存储和传输过程中不能被偶然或蓄意修改、删除、伪造、添加、破坏或丢失，信息在存储和传输过程中必须保持原样。信息完整性表明了信息的可靠性、正确性、有效性和一致性，只有完整的信息才是可信任的信息。
- 可用性（availability）：保证网络资源随时可被合法用户访问，是信息资源容许授权用户按需访问的特性。

- 有效性：是信息系统面向用户服务的安全特性。信息系统只有持续有效，授权用户才能随时随地根据自己的需要访问信息系统提供的服务。

完整的网络信息安全体系至少应包括三类措施：

- 社会的法律政策、安全的规章制度以及安全教育等外部软环境。
- 技术方面的措施，如防火墙技术、网络防毒、信息加密存储与通信、身份验证、授权等。
- 审计和管理措施，同时包含了技术与社会措施。

保证网络安全的技术手段主要包括以下几种。

- 信息加密：数据传输加密、数据存储加密、数据完整性鉴别和密钥管理。
- 身份验证和授权管理：实体访问控制、数据访问控制。
- 安全防御：防火墙技术、防病毒技术；网络介质和通信链路的保护。
- 安全审计和管理：网络实时监控、安全策略审计和漏洞扫描。

1.2.2 网络安全体系结构

当前，通用的网络层次标准有 OSI 和 TCP/IP 两种。OSI 是理论标准；TCP/IP 是工业的事实标准。由于不同的局域网有不同的网络协议，为了使不同的网络能够互联，必须建立统一的网络互联协议。为此，ISO（国际标准化组织）提出了网络互联协议的基本框架，称为开放系统互连（OSI）参考模型。它将整个网络的功能划分为七个层次（如表 1.1 所示）。应用层、表示层、会话层、传输层被归为高层；而网络层、数据链路层、物理层被归为低层。高层负责主机之间的数据传输；低层负责网络数据传输。

表 1.1　网络体系层次

<table>
<tr><th>OSI 模型</th><th>主 要 功 能</th><th>常见协议</th><th>TCP/IP 网络</th><th>主 要 功 能</th><th>常见协议</th></tr>
<tr><td>应用层</td><td>提供应用程序间的通信</td><td>HTTP、FTP</td><td rowspan="3">应用层</td><td rowspan="3">提供应用程序接口</td><td rowspan="3">HTTP、FTP</td></tr>
<tr><td>表示层</td><td>数据格式、数据加密</td><td>NBSSL、LPP</td></tr>
<tr><td>会话层</td><td>建立、维护、管理会话</td><td>RPC、LDAP</td></tr>
<tr><td>传输层</td><td>建立主机端到端连接</td><td>TCP、UDP</td><td>传输层</td><td>建立端到端连接</td><td>TCP、UDP</td></tr>
<tr><td>网络层</td><td>寻址和路由选择</td><td>IP、ICMP</td><td>互联网层</td><td>寻址和路由选择</td><td>IP、ICMP</td></tr>
<tr><td>数据链路层</td><td>介质访问和链路管理</td><td>PPP</td><td rowspan="2">网络接口层</td><td rowspan="2">二进制数据流传输和物理介质访问</td><td rowspan="2">PPP</td></tr>
<tr><td>物理层</td><td>比特流传输</td><td></td></tr>
</table>

层与层之间的联系是通过各层之间的接口来进行的，上层通过接口向下层提出服务请求，而下层通过接口向上层提供服务。除物理层之外，各对等层之间均不存在直接的通信关系，而是通过各对等层之间的通信协议来进行通信；只有两物理层之间通过传输介质进行真正的数据通信。

1.2.2.1 OSI 参考模型

OSI 参考模型是研究、设计新的计算机网络系统和评估、改进现有系统的理论依据，

是理解和实现网络安全的基础。在 OSI 参考模型中主要包括安全服务(security service)、安全机制(security mechanism)和安全管理(security management)。

网络的安全服务包括以下内容。

- 对等实体认证服务:实体的合法性、真实性确认。
- 访问控制服务:防止对任何资源的非授权访问。
- 数据保密服务:加密保护,防止被截获的数据泄密。
- 数据完整性服务:使消息的接收者能够发现消息是否被修改,是否被攻击者用假消息换掉。
- 数据源点认证服务:数据来自真正的源点,以防假冒。
- 信息流安全服务:通过流量填充阻止非法流量分析。
- 不可否认服务:防止对数据源以及数据提交的否认。

为了实现这些安全服务,需要一系列安全机制作为支撑,如下所示。

- 加密机制:应用现代密码学理论,确保数据的机密性。
- 数字签名机制:保证数据完整性和不可否认性。
- 访问控制机制:与实体认证相关,且要牺牲网络性能。
- 数据完整性机制:保证数据在传输过程中不被非法入侵篡改。
- 认证交换机制:实现站点、报文、用户和进程认证等。
- 流量填充机制:针对流量分析攻击而建立的机制。
- 路由控制机制:可以指定数据通过网络的路径。
- 公证机制:用数字签名技术由第三方来提供公正仲裁。

1.2.2.2 网络安全控制系统

通过对网络应用的全面了解,按照安全风险、需求分析结果、安全策略以及安全目标,安全控制系统可以分为物理安全、系统安全、网络安全、应用安全、管理安全等几个方面。

1. 物理安全

物理安全是保障整个网络系统安全的前提,保护计算机网络的物理通路不被损坏、不被窃听以及不被攻击和干扰。它包括三个方面:环境安全、设备安全、媒体安全。防范措施包括:对重要信息存储、收发部门进行屏蔽处理,防止信号外泄;对局域网传输线路传输辐射的抑制;对终端设备辐射的防范。

2. 系统安全

系统安全包括网络结构安全、操作系统安全和应用系统安全。网络结构安全指网络拓扑结构是否合理,线路是否有冗余,路由是否冗余,防止单点失败等。安全防范策略包括:尽量采用安全性较高的网络操作系统并进行必要的安全配置;关闭不常用却存在安全隐患的应用;对保存有用户信息及其口令的关键文件使用权限进行严格限制;通过配备安全扫描系统对操作系统进行安全性扫描,及时发现安全漏洞;应用服务器应关闭一些不经常使用的协议及协议端口号,加强身份认证,严格限制登录者的操作权限。

3. 网络安全

网络安全是整个安全解决方案的关键,通过访问控制、通信保密、入侵检测、网络安全扫描系统、防病毒工具等措施保障。隔离与访问控制可通过严格的管理制度划分虚拟子

网(VLAN)、配备防火墙来进行;防火墙是实现网络安全最基本、最经济、最有效的安全措施之一,它通过制定严格的安全策略实现内外网络或内部网络不同信任域之间的隔离与访问控制;通信保密使得数据以密文形式在网络上传输,可以选择链路层加密和网络层加密等方式;入侵检测是根据已有攻击手段的信息代码对所有网络操作行为进行实时监控、记录,并按制定的策略予以响应,从而防止针对网络的攻击与犯罪行为;网络安全扫描系统可以对网络中所有部件(Web 站点、防火墙、路由器、TCP/IP 及相关协议服务)进行攻击性扫描、分析和评估,发现并报告系统存在的弱点和漏洞,评估安全风险,提出补救措施;病毒防护也是网络安全建设的重要环节之一,反病毒技术包括预防病毒、检测病毒和杀毒三种技术。

4. 应用安全

应用安全表现在内部网络系统中资源共享和信息存储等方面。严格控制内部员工对网络共享资源的使用,在内部子网中一般不开放共享目录,对有经常交换信息需求的用户,在共享时必须加装口令认证机制。对数据库服务器中的数据库必须做安全备份,通过网络备份系统,也可以进行远程备份存储。

5. 安全管理

通过制定健全的安全管理体制、构建安全管理平台、增强人员的安全防范意识,是网络安全得以实现的重要保证;应经常对人员进行网络安全防范意识的培训,全面提高人员的网络安全防范意识;组建安全管理子网,安装集中统一的安全管理软件,如病毒软件管理系统、网络设备管理系统以及网络安全设备统一管理软件,通过安全管理平台实现全网的安全管理。

1.2.2.3 安全体系设计

安全体系设计原则包括以下几个方面:

(1) 需求、风险、代价平衡分析的原则。对任一网络来说,绝对安全难以达到。要进行实际分析,对网络面临的威胁及可能承担的风险进行定性与定量相结合的分析,制定规范和措施,确定系统安全策略。

(2) 一致性原则。一致性原则是指网络安全问题应与网络的生命周期并存,制定的安全体系结构必须与网络的安全需求相一致。

(3) 易操作性原则。安全措施要具有便利性和可操作性,考虑管理人员的自身素质,对操作人员的要求不宜过高。

1.2.2.4 网络安全策略

网络安全策略应考虑安全管理策略和安全技术实施策略两个方面。

(1) 管理策略。即使是最好的、最值得信赖的系统安全措施,也不能完全由计算机系统来独立完成,需要建立完备的安全组织和管理制度,以约束操作人员。

(2) 技术策略。要针对网络、操作系统、数据库、信息共享授权提出具体的措施。

计算机信息系统的安全管理主要基于三个原则,即多人负责原则、任期有限原则、职责分离原则。由于网络互联在链路层、网络层、传输层、应用层等不同协议层均有体现,且

各个层的功能和安全特性不同,因而其网络安全措施也不相同。

物理层安全涉及传输介质的安全特性,抗干扰、防窃听是物理层安全措施制定的重点。

在链路层,可以通过建立虚拟局域网,对物理和逻辑网段进行有效的分割和隔离,消除不同安全级别逻辑网段间的窃听风险。

在网络层,可通过对不同子网的定义和对路由器的路由表控制来限制子网间的通信;同时,利用网关的安全控制能力,限制节点的通信和应用服务,加强对外部用户的识别和验证能力。

1.2.3 网络安全评价标准

评价标准中比较流行的是1985年美国国防部制定的可信任计算机标准评价准则,各国根据自己的国情也都制定了相关的标准。

1.2.3.1 中国评价标准

在我国,1999年10月经过国家质量技术监督局批准发布的《计算机信息系统安全保护等级划分准则》将计算机安全保护划分为以下五个级别:

第1级为用户自主保护级(GB1安全级),它的安全保护机制使用户具备自主安全保护的能力,保护用户的信息免受非法的读写破坏。

第2级为系统审计保护级(GB2安全级),除具备第一级所有的安全保护功能外,要求创建和维护访问的审计跟踪记录,使所有的用户对自己的行为的合法性负责。

第3级为安全标记保护级(GB3安全级),除继承前一个级别的安全功能外,还要求以访问对象标记的安全级别限制访问者的访问权限,实现对访问对象的强制保护。

第4级为结构化保护级(GB4安全级),在继承前面安全级别安全功能的基础上,将安全保护机制划分为关键部分和非关键部分,对关键部分直接控制访问者对访问对象的存取,从而加强系统的抗渗透能力。

第5级为访问验证保护级(GB5安全级),这一级别特别增设了访问验证功能,负责仲裁访问者对访问对象的所有访问活动。

从20世纪80年代中期开始,我国自主制定和采用了一批相应的信息安全标准。但是,应该承认,标准的制定需要较为广泛的应用经验和较为深入的研究背景。这两方面的差距,使我国的信息安全标准化工作与国际已有的工作相比,覆盖的范围还不够大,宏观和微观的指导作用也有待进一步增强。

1.2.3.2 国际评价标准

美国国防部开发的计算机安全标准——可信任计算机标准评价准则(Trusted Computer Standards Evaluation Criteria,TCSEC),即网络安全橙皮书,自从1985年成为美国国防部的标准以来,一直是评估多用户主机和小型操作系统的主要方法。其他子系统(如数据库和网络)也一直用橙皮书来解释评估。橙皮书把安全的级别从低到高分成四个类别:D类、C类、B类和A类,每类又分几个级别,如表1.2所示。

表 1.2　网络安全评价级别

类别	级别	名　称	主要特征
D	D	低级保护	没有安全保护
C	C1	自主安全保护	自主存储控制
	C2	受控存储控制	单独的可查性，安全标识
B	B1	标识的安全保护	强制存取控制，安全标识
	B2	结构化保护	面向安全的体系结构，较好的抗渗透能力
	B3	安全区域	存取监控、高抗渗透能力
A	A	验证设计	形式化的最高级描述和验证

D 级是最低的安全级别，拥有这个级别的操作系统就像一个门户大开的房子，任何人都可以自由进出，是完全不可信任的。对于硬件来说，没有任何保护措施，操作系统容易受到损害，没有系统访问限制和数据访问限制，任何人不需任何账户都可以进入系统，访问他人的数据文件不受任何限制。属于这个级别的操作系统有 DOS 和 Windows 98 等。

C1 是 C 类的一个安全子级。C1 又称选择性安全保护（discretionary security protection）系统，它描述了一个典型的用在 UNIX 系统上的安全级别。这种级别的系统对硬件有某种程度的保护，如用户拥有注册账号和口令，系统通过账号和口令来识别用户是否合法，并决定用户对程序和信息拥有何种访问权限，但硬件受到损害的可能性仍然存在。

C2 级除了包含 C1 级的特征外，还具有访问控制环境（controlled access environment）权力，即具有进一步限制用户执行某些命令或者访问某些文件的权限，而且还加入了身份认证等级。另外，系统对事件进行审计，并写入日志中，如何时开机，用户在何时何地登录系统等，通过查看日志，就可以发现入侵痕迹。审计除了可以记录下系统管理员执行的活动以外，还加入了身份认证级别，缺点在于它需要额外的处理时间和磁盘空间。

使用附加身份验证就可以让一个 C2 级系统用户在不是超级用户的情况下有权执行系统管理任务。授权分级使系统管理员能够给用户分组，授予他们访问某些程序的权限或访问特定的目录。能够达到 C2 级别的常见操作系统有 UNIX 系统、Novell 3.X 或者更高版本、Windows NT、Windows 2000 和 Windows 2003。

B 级中有三个级别。B1 级即标志安全保护（labeled security protection），是支持多级安全（例如秘密和绝密）的第一个级别，这个级别说明处于强制性访问控制之下的对象，系统不允许文件的拥有者改变其许可权限。这种安全级别的计算机系统一般在政府机构中，比如国防部和国家安全局的计算机系统。

B2 级又叫结构保护（structured protection）级别，它要求计算机系统中所有的对象都要加上标签，而且给设备（磁盘、磁带和终端）分配单个或者多个安全级别。

B3 级又叫安全域（security domain）级别，使用安装硬件的方式来加强域的安全，例如，内存管理硬件用于保护安全域免遭无授权访问或更改其他安全域的对象。该级别也要求用户通过一条可信任途径连接到系统上。

A 级又称验证设计(verified design)级别，是当前橙皮书的最高级别，它包含了一个严格的设计、控制和验证过程。安全级别设计必须从数学角度上进行验证，而且必须进行秘密通道和可信任分布分析。

可信任分布(trusted distribution)的含义是：硬件和软件在物理传输过程中受到保护，以防止破坏安全系统。

1.2.4 信息安全定义

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，免受破坏、更改和泄露，系统连续可靠正常地运行，信息服务不中断。信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

随着信息安全技术的发展，经历了从基本安全隔离、主机加固阶段，到后来的网络认证阶段，直到将行为监控和审计也纳入安全的范畴。这样的演变不仅仅是为了避免恶意攻击，更重要的是为了提高网络的可信度。

信息安全的内涵在不断的延伸，从最初的信息保密性发展到信息的完整性、可用性、可控性和不可否认性，进而又发展为“攻(攻击)、防(防范)、测(检测)、控(控制)、管(管理)、评(评估)”等多方面的基础理论和实施技术。

从广义上讲，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。目前常用的基础性安全技术包括以下内容。

- 身份认证技术：用来确定用户或者设备身份的合法性，典型的手段有口令、身份识别、PKI 证书和生物认证等。
- 加解密技术：在传输过程或存储过程中进行信息数据的加解密，典型的加密体制有对称加密和非对称加密。
- 边界防护技术：防止外部网络用户以非法手段进入内部网络，保护内部网络操作环境，典型的设备有防火墙和入侵检测设备。
- 访问控制技术：保证网络资源不被非法使用和访问。访问控制是网络安全防范和保护的主要核心策略，在身份识别的基础上，根据身份对提出资源访问的请求加以权限控制。
- 主机加固技术：主机加固技术对操作系统、数据库等进行漏洞加固和保护，提高系统的抗攻击能力。
- 安全审计技术：包含日志审计和行为审计。通过日志审计协助管理员评估网络配置的合理性、安全策略的有效性；通过对用户的网络行为审计，确认行为的合规性，确保管理的安全。

随着信息网络的不断普及，网络攻击手段也在不断复杂化、多样化，随之产生的信息安全技术和解决方案也在不断发展变化，安全产品和解决方案也更趋于合理化、适用化。经过多年的发展，安全防御体系已由“被动防范”向“主动防御”发展，由“保护网络”向“保护资产”过渡，并逐步构建出具有可防、可控、可信特点的信息网络架构。

1.3 网络安全实验基本要求

1. 实验目的

通过网络安全实验使学生掌握网络安全技术的基本概念、原理和技术，了解基本的网络安全攻防技术、常用工具的使用方法及原理，加深对课堂理论教学的理解，培养学生的实验技能、动手能力和分析问题、解决问题的能力。

2. 实验要求

通过本实验的学习，学生应达到以下基本要求：

（1）了解计算机网络安全的重要性以及相关的法律法规，建立网络安全意识。

（2）掌握计算机网络安全方面的基本技术，能对系统的安全问题做出相应对策。

（3）掌握网络安全的防范技术和防计算机病毒技术。

3. 实验内容

本实验所规划的实验项目内容、学时分配、实验类型及综合要求情况如表 1.3 所示。

表 1.3 实验项目建议内容

序号	基本实验内容	建议学时	内容提要	实验类型	实验要求
1	网络分析器应用实验	4	熟悉并熟练运用网络分析器，能够对局域网的数据进行分析	综合性	撰写网络分析测试分析报告
2	剖析远程控制程序	2	了解远程控制的基本原理，熟悉远程控制软件的使用	综合性	编写一个远程控制程序
3	SSL、VPN 应用与实践	2	了解 SSL、VPN 技术及其构建网络安全防护的基本机制与模式	综合性	利用 VPN 技术实现远程访问
4	防火墙技术	2	熟悉防火墙基本知识，了解防火墙的具体使用，熟悉防火墙配置规则，掌握防火墙的基本原理和作用	综合性	撰写防火墙技术分析报告
5	入侵检测系统分析与应用	2	了解入侵检测系统，熟悉入侵检测软件的使用	综合性	撰写入侵检测系统应用报告
6	虚拟蜜罐分析与实践	4	掌握虚拟蜜网的定义、结构及具体搭建环境和步骤	综合性	利用蜜网分析网络访问行为

第 2 章　网络安全研究内容

2.1　密码技术

2.1.1　基本概念

密码学(cryptology)一词是由希腊字根“隐藏”(Kryptós)及“信息”(lógos)组合而成，泛指一切关于研究密码通信的研究内容。密码具有信息加密、可鉴别性、完整性、抗抵赖性等作用。密码学是研究编制密码和破译密码的技术科学。研究密码变化的客观规律，应用于编制密码以保守通信秘密的，称为编码学；应用于破译密码以获取通信情报的，称为破译学。编码学和破译学总称密码学。

密码是通信双方按约定的法则进行信息特殊变换的一种重要保密手段。依照这些法则，变明文为密文，称为加密变换；变密文为明文，称为解密变换。密码在早期仅对文字或数码进行加、解密变换，随着通信技术的发展，对语音、图像、数据等都可实施加、解密变换。密码学是在编码与破译的斗争实践中逐步发展起来的，并随着先进科学技术的应用，已成为一门综合性的尖端技术科学。

密码体制也称为密码系统，是指能完整地解决信息安全性中机密性、数据完整性、认证、身份识别、可控性及不可抵赖性等问题中的一个或者多个的完整系统。对一个密码体制的正规描述，需要用数学方法清楚地描述其中的各种对象、参数、解决问题所使用的算法等。

2.1.2　密码算法

在网络安全领域常见的加密算法有以下几种。

1. DES 算法

DES 算法属于密码体制中的对称密码体制，又被称为美国数据加密标准，是 1972 年美国 IBM 公司研制的对称密码体制加密算法。其密钥长度为 56 位，明文按 64 位进行分组，将分组后的明文根据 56 位的密钥按位替代或交换的方法形成密文。

算法特点：分组较短，密钥太短，密码生命周期短，运算速度较慢。DES 的入口参数有三个：Key、Data、Mode。Key 为加密解密使用的密钥；Data 为加密解密的数据；Mode 为其工作模式。当工作模式为加密模式时，明文按照 64 位进行分组，形成明文组，Key 用于对数据加密；当工作模式为解密模式时，Key 用于对数据解密。实际应用中，密钥只用到了 64 位中的 56 位，这样才具有高的安全性。

2. AES(advanced encryption standard，高级加密标准)算法

AES 算法是下一代的加密算法标准，速度快，安全级别高。2000 年 10 月，NIST(美国国家标准和技术协会)从 15 种候选算法中选出 AES 算法作为新的密钥加密标准。

AES 算法正日益成为电子数据加密的实际标准。

AES 是一个迭代的、对称密钥分组的密码，它可以使用 128 位、192 位和 256 位密钥，并且用 128 位（16 字节）分组加密和解密数据。AES 算法基于排列和置换运算，该算法利用分组密码返回的加密数据的位数与输入数据相同的特点，使用循环结构进行迭代加密，在该循环中重复置换和替换输入数据。

3. ECC 算法

ECC 算法又称椭圆曲线加密系统，是目前已知的所有公钥密码体制中能够提供最高比特强度的一种公钥体制。

椭圆曲线密码体制具有以下优点：

（1）用椭圆曲线来构造密码体制，用户可以任意地选择安全的椭圆曲线，在确定了有限域后，椭圆曲线的选择范围很大。

（2）一旦选择恰当的椭圆曲线，就没有有效的指数算法来攻击它。

2.1.3 网络安全应用

密码学在网络安全中的具体应用主要包括以下几种形式。

（1）由于加密算法强度较弱，而遭受到网络安全攻击，主要包括：①侦听并解读明文数据通信流，窃取敏感数据；②对于捕获到的数据包，进行恶意篡改；③窃取合法用户的访问口令，对目标系统进行攻击；④直接窃取加密密钥。

（2）用于认证服务，使网络上的用户可以相互证明自己的身份，即能正确对信息进行解密的用户就是合法用户。用户在对应用服务器进行访问前，必须从第三方获取该应用服务器的访问许可证。

（3）用于提高电子邮件的安全性。目前，电子邮件广泛应用的保密方法是 PGP（pretty good privacy），PGP 采用的解决方案是给每个公钥分配一个密钥标识，并在很大概率上与用户标识一一对应。发送方需要使用一个私钥加密消息摘要，接收方必须知道应使用哪个公钥解密。相应地，消息的数字签名部分必须包括公钥对应的 64 位密钥标识。当接收到消息后，接收方用密钥标识指示的公钥验证签名。

密码技术并不能解决所有的网络安全问题，它需要与信息安全的其他技术如访问控制技术、网络监控技术等互相融合，形成综合的信息网络安全保障。

2.2 防火墙技术

防火墙技术是建立在现代通信网络技术和信息安全技术基础上的应用性安全技术，越来越多地应用于专用网络与公用网络的互联环境之中。防火墙本身具有较强的抗攻击能力，它是提供信息安全服务，实现网络和信息安全的基础设施。防火墙具有以下特征：

- 网络位置特性。内部网络和外部网络之间的所有网络数据都必须经过防火墙。
- 工作原理特性。只有符合安全策略的数据才能通过防火墙。
- 先决条件。防火墙自身应具有非常强的抗攻击能力。

2.2.1　防火墙体系结构

防火墙的四种基本体系结构包括屏蔽路由器、双穴主机网关、屏蔽主机网关、被屏蔽子网(非军事区 DMZ)。

典型的实用防火墙包括三种。

1. 包过滤路由器防火墙

包过滤路由器是一种便宜、简单、常见的防火墙。包过滤路由器在网络之间完成数据包转发的普通路由功能,并利用包过滤规则来允许或拒绝数据包。其结构如图 2.1 所示。

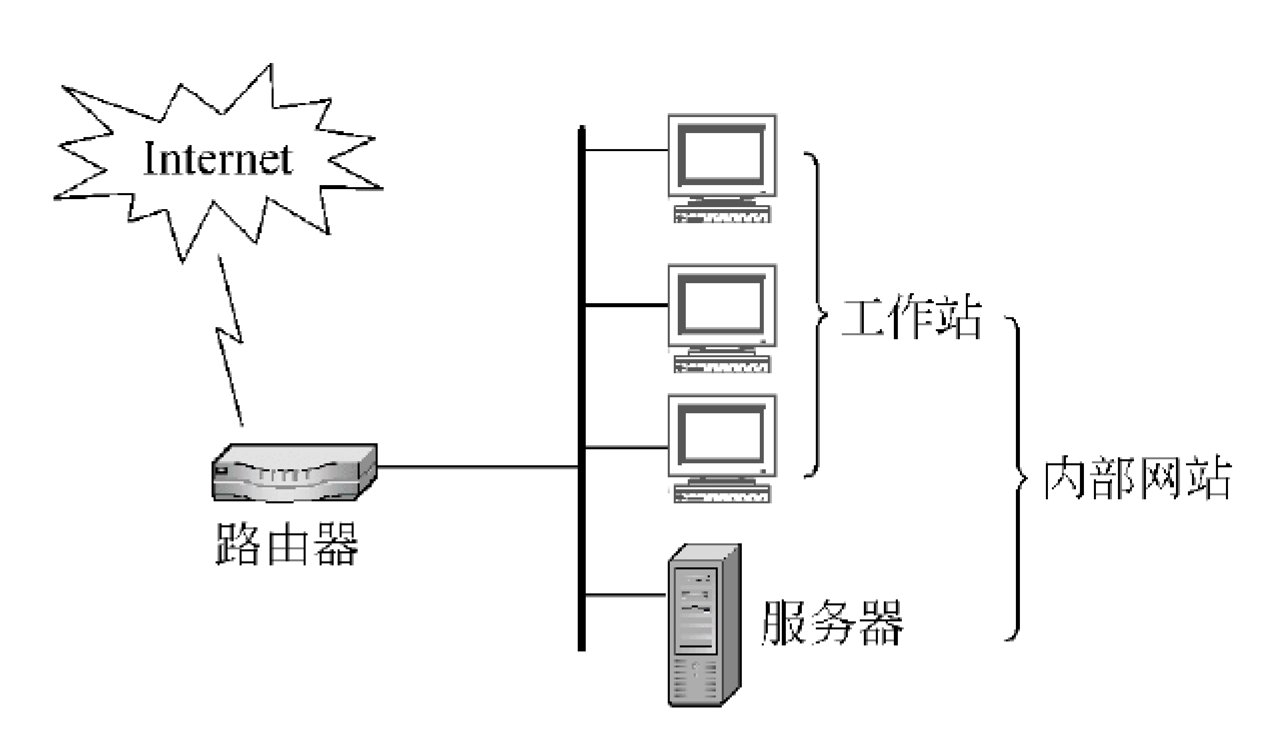


图 21　包过滤路由器防火墙

尽管这种防火墙系统有价格低和易于使用的优点,但同时也有缺点,如配置不当的路由器可能受到攻击,以及利用包裹在允许服务和系统内的操作进行攻击等。由于允许在内部和外部系统之间直接交换数据包,因此攻击面可能会扩展到所有主机和路由器所允许的全部服务上。另外,如果有一个包过滤路由器被渗透,则内部网络上的所有系统都可能受到损害。

2. 屏蔽主机防火墙

屏蔽主机防火墙系统采用了包过滤路由器和堡垒主机,如图 2.2 所示。这个防火墙系统提供的安全等级比包过滤路由器要高,因为它实现了网络层安全(包过滤)和应用层安全(代理服务),所以入侵者在破坏内部网络的安全性之前,必须首先渗透两种不同的安全系统。

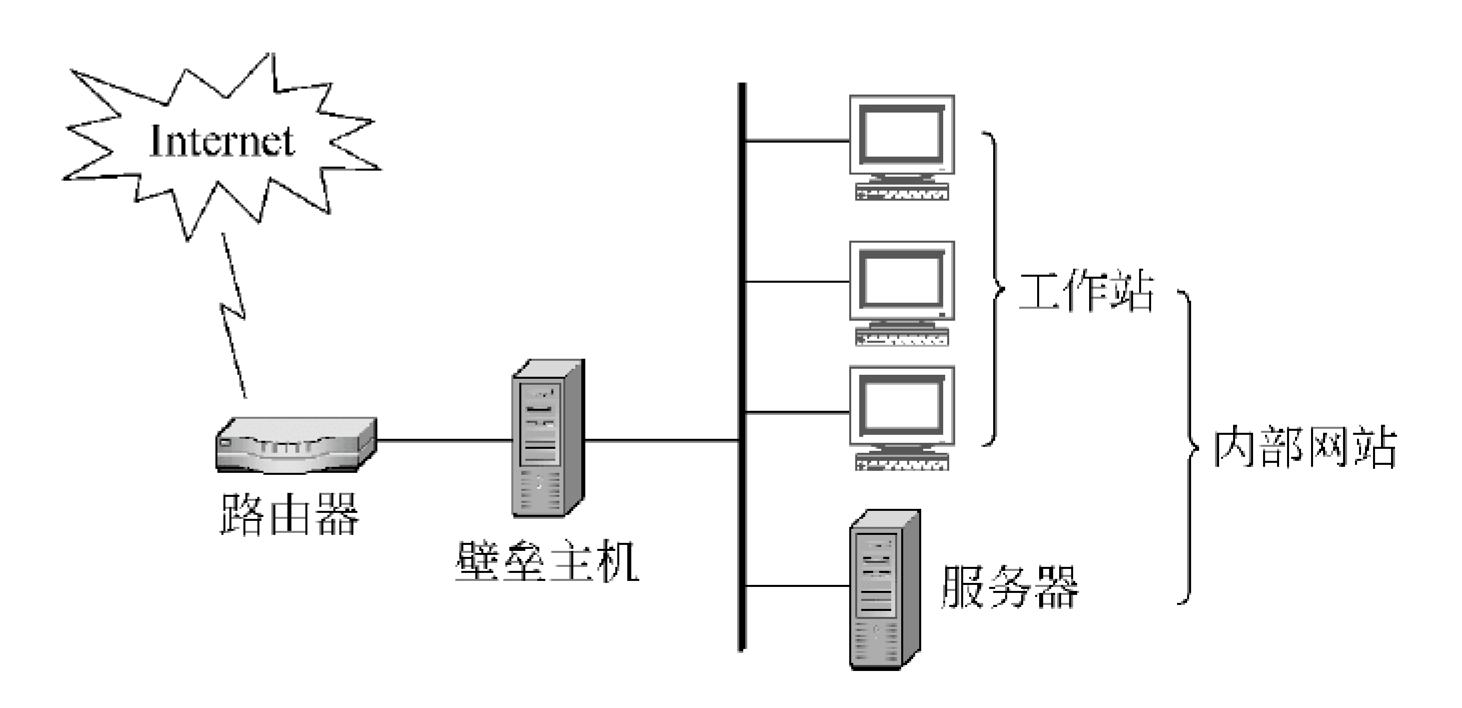


图 22　屏蔽主机防火墙 (单堡垒主机)

对于这种防火墙系统，堡垒主机配置在内部网络上，而包过滤路由器则放置在内部网络和外部网络之间。在路由器上进行规则配置，使得外部系统只能访问堡垒主机，去往内部系统上其他主机的信息全部被阻塞。由于内部主机与堡垒主机处于同一个网络，内部系统是否允许直接访问外部网络，或者是要求使用堡垒主机上的代理服务来访问外部网络，全部由安全策略来决定。对路由器的过滤规则进行配置，使得其只接受来自堡垒主机的内部数据包，并强制内部用户使用代理服务。

如图 2.3 所示，用双宿堡垒主机甚至可以构造更加安全的防火墙系统。这种物理结构强行让所有去往内部网络的信息经过堡垒主机，由于堡垒主机是唯一能从外部网络上直接访问的内部系统，因此有可能受到攻击的主机就只有堡垒主机本身。但是，如果允许用户注册到堡垒主机，那么整个内部网络上的主机都会受到攻击的威胁。牢固可靠、避免被渗透和不允许用户注册对堡垒主机来说是至关重要的。

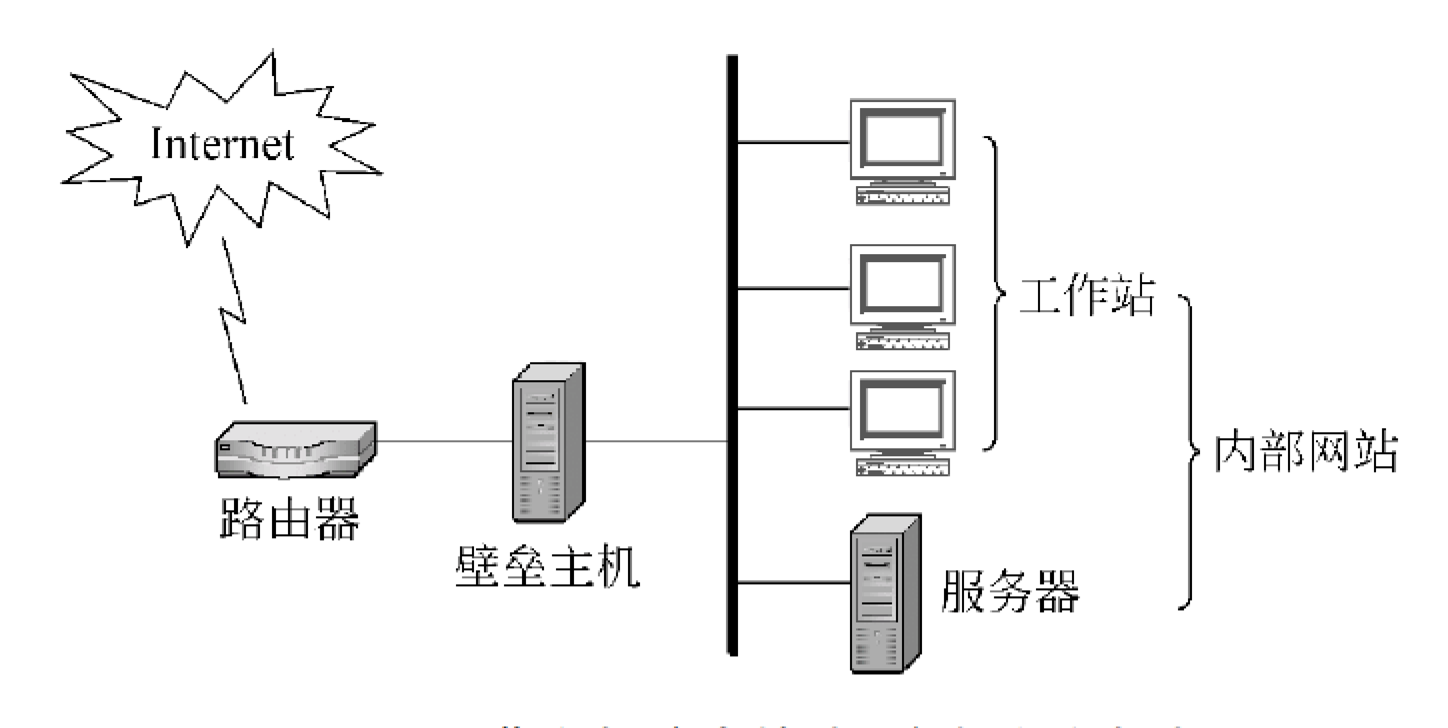


图 23　屏蔽主机防火墙（双宿堡垒主机）

3. 屏蔽子网防火墙

屏蔽子网防火墙采用了两个包过滤路由器和一个堡垒主机，如图 2.4 所示。这个防火墙系统建立的是最安全的防火墙系统，因为在定义了“非军事区”（DMZ）网络后，它支持网络层和应用层安全功能。网络管理员将堡垒主机、信息服务器、Modem 组以及其他公用服务器放在 DMZ 网络中。通过 DMZ 网络直接进行信息传输是严格禁止的。

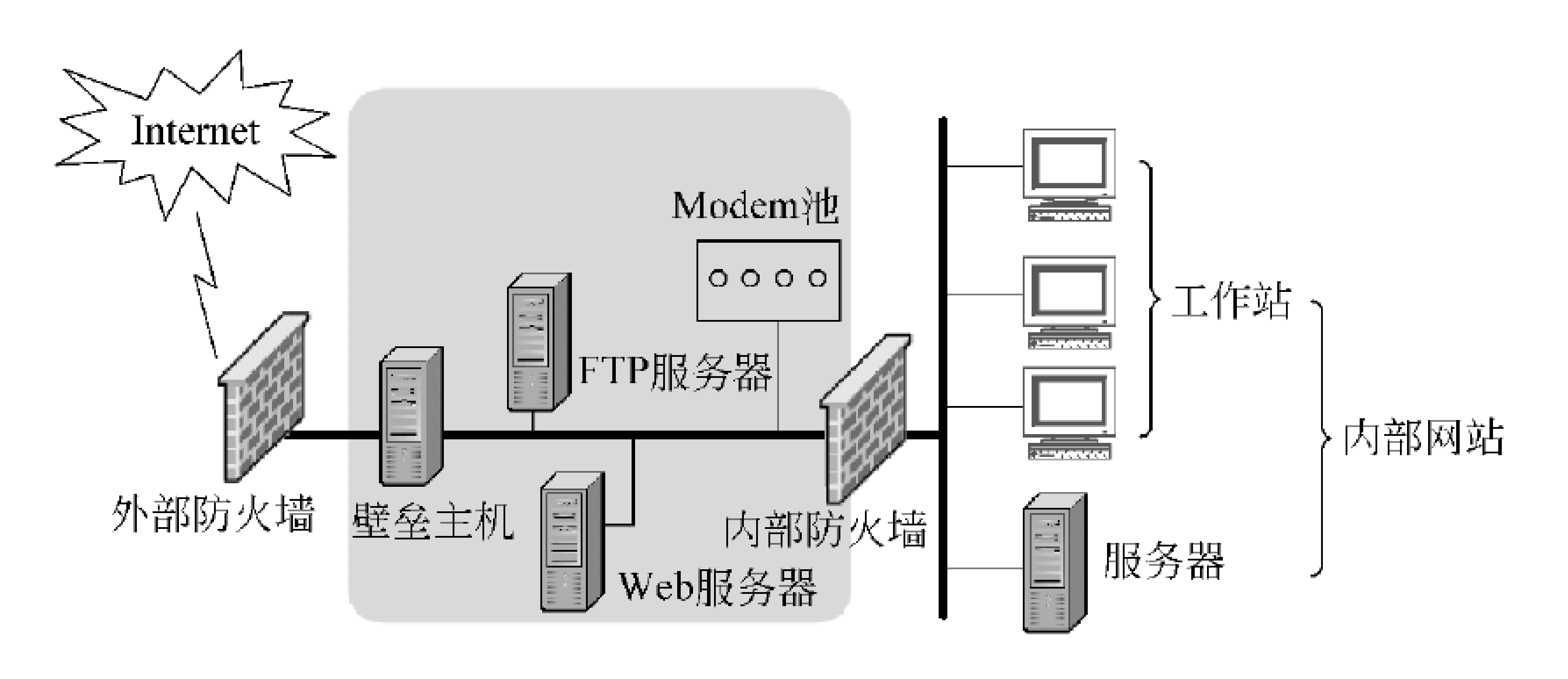


图 24　屏蔽子网防火墙

外部路由器用于防范通常的外部攻击（如源地址欺骗和源路由攻击），并管理外部网络到 DMZ 网络的访问。它只允许外部系统访问堡垒主机。内部路由器则提供第二层防御，只接受来自堡垒主机的数据包，负责管理 DMZ 到内部网络的访问。

部署屏蔽子网防火墙系统有如下几个特别的好处：

(1) 入侵者必须突破三个不同的设备才能侵袭内部网络：外部路由器、堡垒主机以及内部路由器。

(2) 由于外部路由器只能向外部网络通告 DMZ 网络的存在，这样网络管理员就可以保证内部网络是“不可见”的；由于内部路由器只向内部网络通告 DMZ 网络的存在，内部网络上的系统不能直接通往外部网络，这样就保证了内部网络上的用户必须通过驻留在堡垒主机上的代理服务才能访问外部网络。

2.2.2 包过滤防火墙

包过滤防火墙工作在 OSI 网络参考模型的网络层和传输层，它根据数据包头的源地址、目的地址、端口号和协议类型等标志确定数据流是否允许通过，如图 2.5 所示。

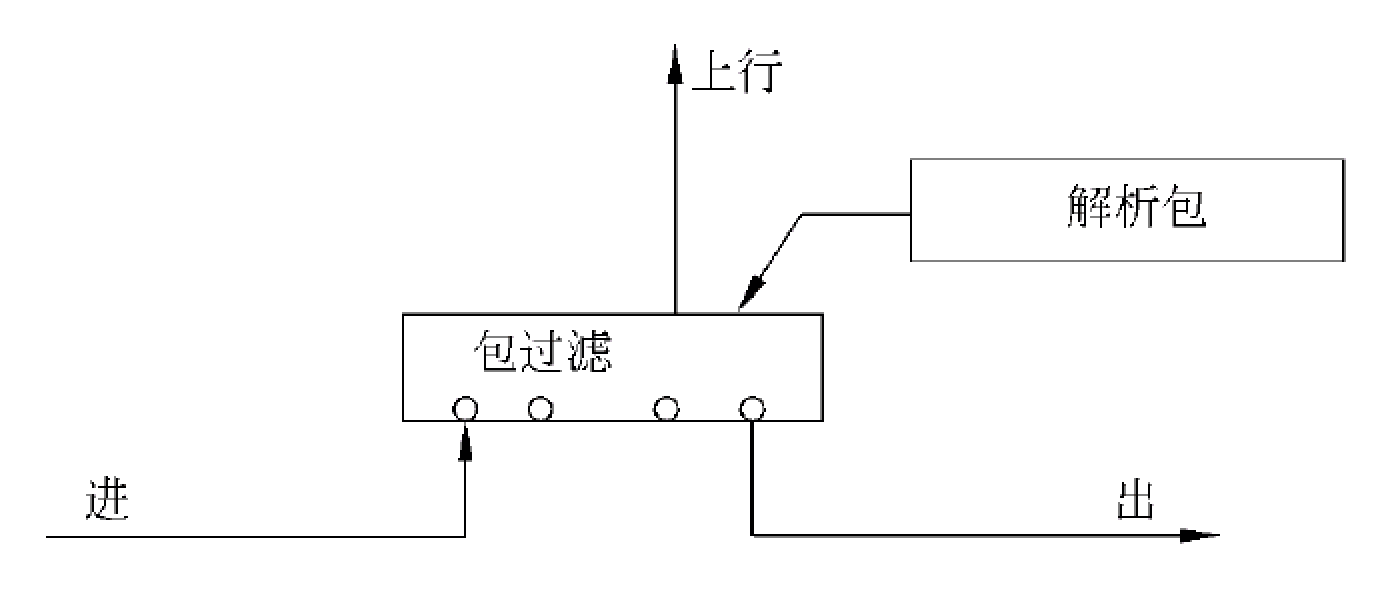


图 25 包过滤防火墙结构

包过滤是一种网络安全保护机制，用来控制进出网络的数据流。通过控制存在于某一网段的数据流类型，包过滤技术可以限定存在于某一网段的服务内容，不符合网络安全的服务将被严格限制。基于包中的协议类型和字段值，过滤路由器能够区分数据流量。

包过滤具有以下优点：

- 一个独立的、网络位置适当的包过滤路由器有助于保护整个网络。如果仅有一个路由器连接内部与外部网络，不论内部网络大小、拓扑结构如何，通过单个路由器进行数据包过滤，在网络安全保护上都会取得较好的效果。
- 数据包过滤对用户透明。不同于代理技术，数据包过滤不要求任何自定义配置，也不要求用户进行任何特殊学习。较强的“透明度”是包过滤的一大优势。
- 过滤速度快、效率高。就代理技术而言，包过滤技术只检查报头相应字段，一般不查看数据包的内容，且核心部分是由硬件实现的，故转发速度快、效率高。

包过滤具有以下缺点：

- 不能彻底防止地址欺骗。大多数包过滤技术都是基于源 IP 地址、目的 IP 地址而进行过滤的。而 IP 地址的伪造是很容易、很普遍的，即使按 MAC 地址进行绑定，也是不可信的。对于一些安全性要求较高的网络，包过滤技术无法满足要求。
- 部分应用协议不适合于数据包过滤。RPC、X-Window 和 FTP 等应用协议无法适用于包过滤技术。服务代理和 HTTP 链接也会削弱基于源地址和源端口的过滤功能。

• 数据包过滤技术无法执行某些安全策略。数据包过滤技术所提供的信息不能完全满足人们对安全策略的需求,不能强行限制特殊的用户。同样地,当通过端口号对高级协议强行进行限制时,恶意的知情者能够很容易地破坏这种控制。

从以上分析可以看出,包过滤防火墙技术虽然能确保一定的安全保护,但是作为第一代防火墙技术,本身存在较多缺陷,不能提供较高的安全性。在实际应用中,很少把包过滤技术当做单独的安全解决方案,而是通常把它与其他防火墙技术捆绑使用。

2.2.3 代理防火墙

代理防火墙是一种较新型的防火墙技术,其特点是完全"阻隔"了网络数据流,通过对每种应用服务编制专门的代理程序,实现监视和控制应用层数据流的功能。它分为应用层网关和电路层网关。

代理防火墙工作于应用层,且针对特定的应用层协议。代理防火墙通过软件方式获取应用层通信流量,并在用户层和应用协议层提供访问控制,保持所有应用程序的使用记录。记录和控制所有进出流量的能力是应用层网关的主要优点之一。

如图 2.6 所示,代理服务器作为内部网络客户端的服务器拦截住所有要求,也向客户端转发响应。代理客户(proxy client)负责代表内部客户端向外部服务器发出请求,当然也向代理服务器转发响应。当某用户想和一个运行代理的网络建立联系时,应用层网关会阻塞这个连接,然后对连接请求的各个域进行检查。如果此连接请求符合预定的安全策略或规则,代理防火墙便会在用户和服务器之间建立一个"桥",从而保证其通信。对不符合预定的安全规则的,则阻塞或抛弃。

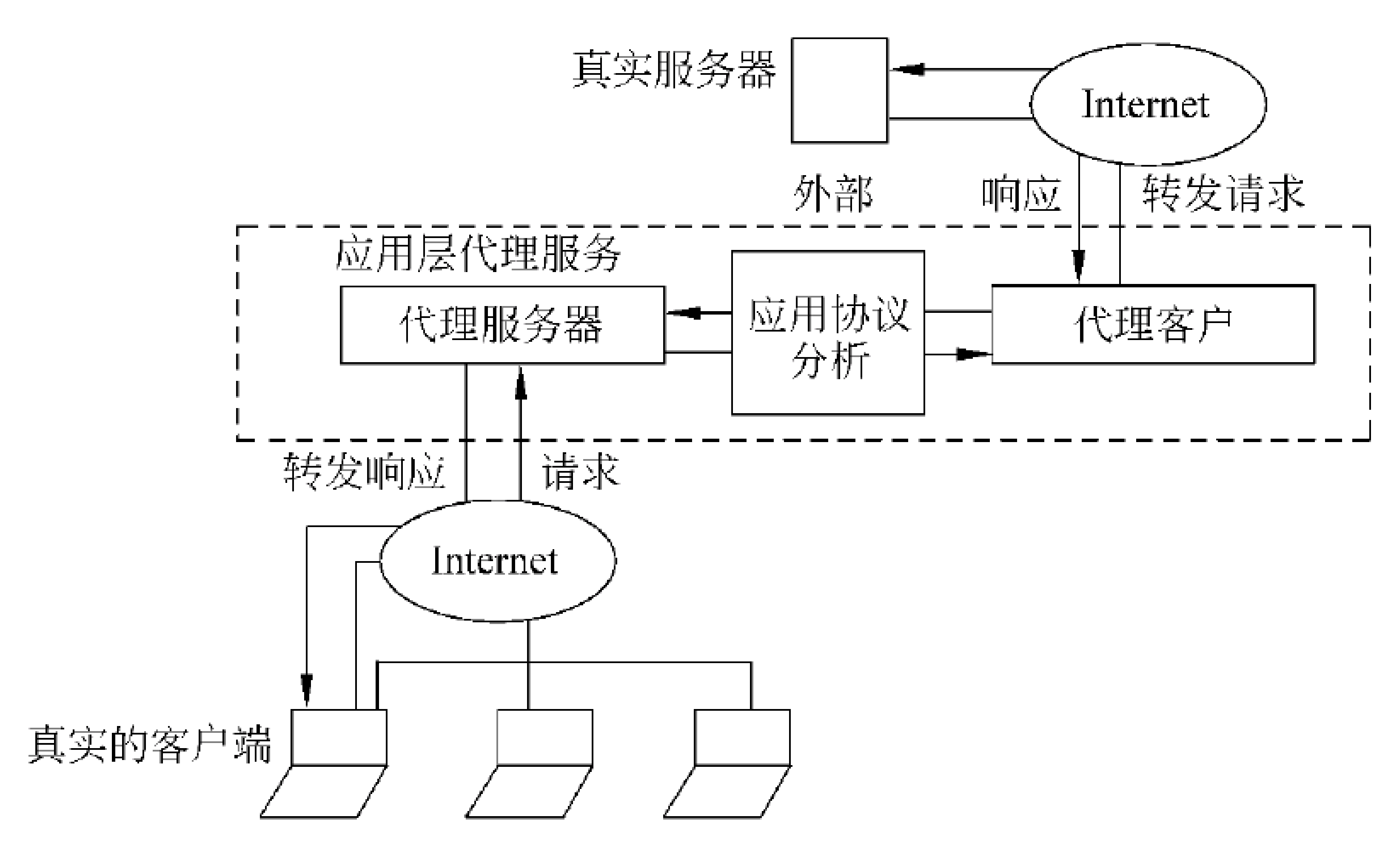


图 26　应用层网关代理技术

另一种类型的代理技术称为电路层网关(circuit gateway)。在电路层网关中,包被提交至用户应用层处理。电路层网关用来在两个通信端之间转换包,如图 2.7 所示。

电路层网关是建立应用层网关的一个更加灵活的方法。在电路层网关中,可能要安装特殊的客户机软件,用户需要一个用户接口来相互作用。

代理防火墙技术具有以下优点:

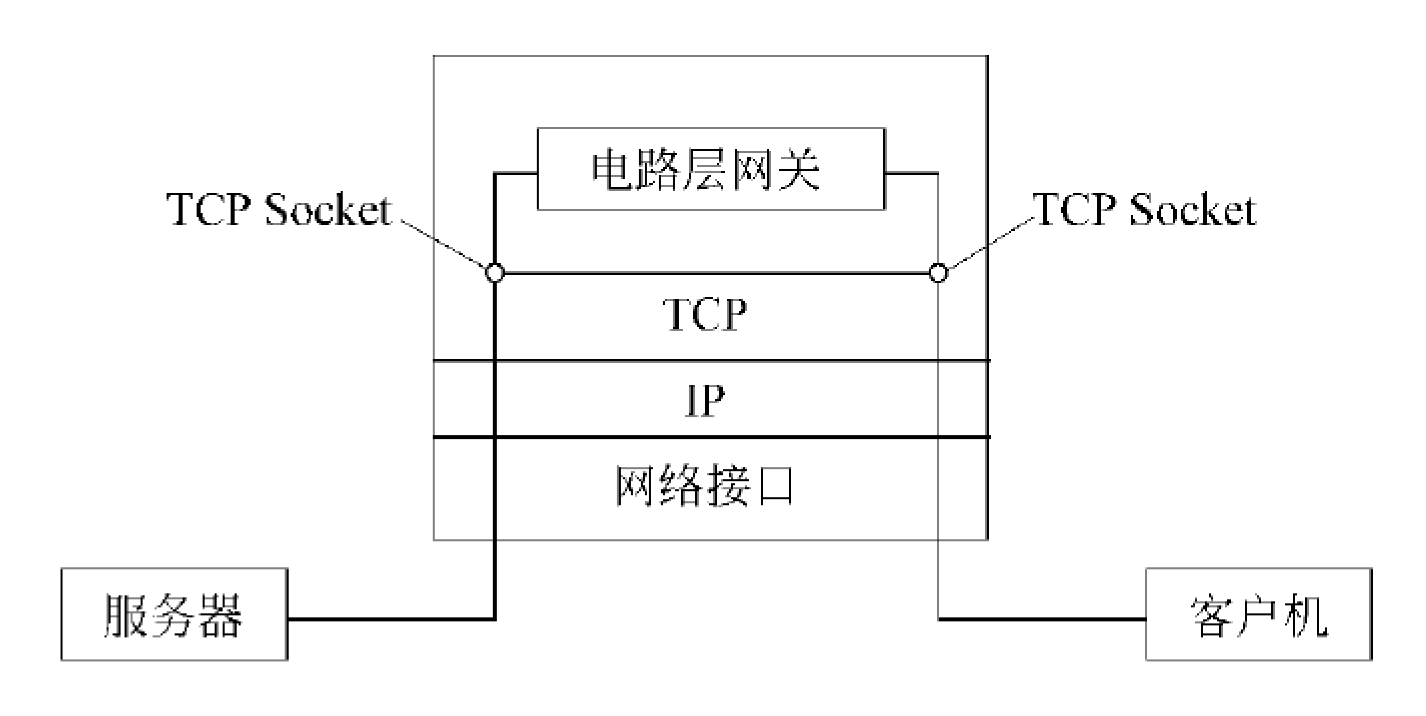


图 27　电路层网关代理技术

• 代理易于配置。由于是软件，所以代理较过滤路由器更易配置。如果代理实现得好，则对配置协议的要求可以低一些，从而避免了配置错误。
• 代理能生成各项记录。代理工作在应用层，它检查各项数据，所以可以生成各项日志、记录。这些日志、记录对于流量分析、安全检验是十分重要的。
• 代理能灵活地控制进出流量。通过采取一定的措施，按照一定的规则，可以借助代理实现一整套的安全策略。
• 代理能过滤数据内容。可以把一些过滤规则应用于代理，让它实现文本过滤、图像过滤、预防病毒或扫描病毒等功能。
• 代理能为用户提供透明的加密机制。代理能够完成加解密的功能，从而确保数据的机密性，这点在虚拟专用网中特别重要。
• 代理可以方便地与其他安全手段集成。目前的安全问题解决方案很多，如认证(authentication)、授权(authorization)、账号(accounting)、数据加密、安全协议(SSL)等。如果将代理与这些手段联合使用，将大大增加网络安全性。

代理防火墙技术具有以下缺点：
• 代理速度较路由器慢。路由器只是简单检查 TCP/IP 报头特定的几个域，不做详细分析、记录。而代理工作于应用层，要检查数据包的内容，按特定的应用协议(如 HTTP)审查、扫描数据包内容，进行代理(转发请求或响应)，速度较慢。
• 代理对用户不透明。许多代理要求用户安装特定客户端软件，这给用户增加了不透明度。安装和配置特定的应用程序既耗费时间，又容易出错。
• 代理服务不能保证免受所有协议弱点的限制。作为一个安全问题的解决方法，代理服务的安全取决于对协议中安全操作的判断能力。每个应用层协议都或多或少存在一些安全问题，对于一个代理服务器来说，要彻底避免这些安全隐患几乎是不可能的，除非关掉这些服务。
• 代理不能改进低层协议的安全性。因为代理工作在 TCP/IP 之上，属于应用层，所以它不能改善低层通信协议的能力。对于 IP 欺骗、SYN 泛滥、伪造 ICMP 消息和一些拒绝服务攻击缺乏必要的抵抗能力和应对机制。而这些方面对于网络的健壮性是相当重要的。

2.3 入侵检测

据统计，全球 80%以上的入侵来自于网络内部。由于性能的限制，防火墙通常不能提供实时的入侵检测能力，对于来自于内部网络的攻击，防火墙形同虚设。入侵检测是对防火墙极其有益的补充。入侵检测系统能在入侵攻击对系统发生危害前检测到入侵攻击，并利用报警与防护系统驱逐入侵攻击。在入侵攻击过程中，能减少入侵攻击所造成的损失。在被入侵攻击后，收集入侵攻击的相关信息，作为防范系统的知识，添加到知识库中，增强系统的防范能力，避免系统再次受到入侵。在不影响网络性能的情况下对网络进行监听，从而提供对内部攻击、外部攻击和误操作的实时监控，大大提高了网络的安全性。

2.3.1 入侵检测技术分类

入侵检测是从计算机网络或计算机系统中的若干关键点搜集信息并对其进行分析，从中发现网络或系统中是否存在违反安全策略的行为和遭到袭击的迹象的一种机制。入侵检测系统使用入侵检测技术对网络与系统进行监视，并根据监视结果采取不同的安全动作，从而最大限度地降低可能的入侵危害。经过几年的发展，入侵检测产品开始步入快速的成长期。

2.3.1.1 基于网络的入侵检测

基于网络的入侵检测产品（NIDS）放置在比较重要的网段内，不停地监视网段中的各种数据包，对数据包进行特征分析。如果数据包与内置的某些规则吻合，入侵检测系统就会发出警报甚至直接切断网络连接。目前，大部分入侵检测产品是基于网络的。值得一提的是，在网络入侵检测系统中，有多个久负盛名的开放源码软件，它们是 Snort、NFR、Shadow 等。

网络入侵检测系统具有以下优点：

- 网络入侵检测系统能够检测来自网络的攻击，特别是越权的非法访问。
- 不需要改变服务器等主机的配置，不占用过多的系统资源，不影响业务系统的性能。
- 发生故障不会影响正常业务的运行，部署一个网络入侵检测系统的风险比主机入侵检测系统的风险少得多。

网络入侵检测系统具有以下弱点：

- 网络入侵检测系统只检查直接连接网段的通信，不能检测在不同网段的网络包。在使用交换以太网的环境中会出现检测范围的局限。而安装多台网络入侵检测系统的传感器会使部署整个系统的成本大大增加。
- 网络入侵检测系统为了性能目标通常采用特征检测的方法，它可以检测出一些简单的普通攻击，而很难检测出一些复杂的需要大量计算与分析时间的攻击。
- 网络入侵检测系统可能会将大量的数据传回分析系统中。在一些系统中监听特定的数据包会产生大量的分析数据流量。这样的系统中，传感器协同工作能力较弱。

- 网络入侵检测系统处理加密的会话过程较困难,目前通过加密通道的攻击尚不多,随着 IPv6 的普及,这个问题会越来越突出。

2.3.1.2 基于主机的入侵检测

基于主机的入侵检测产品(HIDS)通常是安装在被重点监测的主机上,对该主机的网络连接以及系统审计日志进行智能分析和判断。如果其中主体活动十分可疑,入侵检测系统就会采取相应措施。

主机入侵检测系统具有以下优点:

- 主机入侵检测系统与网络入侵检测系统相比通常能够提供更详尽的相关信息。
- 主机入侵检测系统通常情况下比网络入侵检测系统误报率要低,因为检测主机上运行的命令序列比检测网络流更简单,系统的复杂性也少得多。

主机入侵检测系统具有以下弱点:

- 主机入侵检测系统安装在需要保护的设备上,会降低应用系统的效率。安装了主机入侵检测系统后,将把不允许安全管理员访问的服务器变成可以访问的了。
- 主机入侵检测系统依赖于服务器固有的日志与监视能力。如果服务器没有配置日志功能,则必须重新配置,这将会给运行中的业务系统带来不可预见的性能影响。
- 全面部署主机入侵检测系统代价较大,只能选择部分主机保护。那些未安装主机入侵检测系统的机器将成为保护的盲点,入侵者可利用这些机器达到攻击目标。
- 主机入侵检测系统除了监测自身的主机以外,根本不监测网络上的情况。对入侵行为分析的工作量将随着主机数目的增加而增加。

2.3.1.3 混合入侵检测

基于网络的入侵检测产品和基于主机的入侵检测产品都有不足之处,单纯使用一类产品会造成主动防御体系不全面。但是,它们的缺陷是可以互补的。综合基于网络和基于主机两种结构特点的入侵检测系统,既可发现网络中的攻击信息,也可从系统日志中发现异常情况,构架成一套完整立体的主动防御体系,称为混合入侵检测方法。

2.3.1.4 文件完整性检查

文件完整性检查系统检查计算机中的文件变化情况。文件完整性检查系统保存有每个文件的数字文摘数据库,每次检查时,它重新计算文件的数字文摘并将它与数据库中的值相比较,如不同,则文件已被修改,若相同,则文件未发生变化。

文件完整性检查系统具有以下优点:

- 从数学上分析,攻克文件完整性检查系统,无论是时间上还是空间上,都是不可能的。文件完整性检查系统是一个检测系统是否被非法使用的重要工具之一。
- 文件完整性检查系统具有相当的灵活性,可以用于监测系统中所有文件或某些重要文件。

文件完整性检查系统具有以下弱点:

- 文件完整性检查系统依赖于本地的文摘数据库。与日志文件一样,这些数据可能

被入侵者修改。

- 做一次完整的文件完整性检查是一个非常耗时的工作。
- 系统有些正常的更新操作可能会带来大量的文件更新，从而产生比较繁杂的检查与分析工作。

2.3.2 入侵检测系统结构

1980 年 4 月，研究人员在为美国空军提交的一份题为《计算机安全威胁监控与监视》的技术报告中，第一次完整地介绍了入侵检测技术的概念。报告认为这是一种对计算机系统风险和威胁的分类方法，并将威胁分为外部渗透、内部渗透和不法行为三种，还提出了利用审计跟踪数据监视入侵活动的核心思想。

2.3.2.1 入侵检测系统结构

一个入侵检测产品通常由两部分组成：传感器(sensor)与控制台(console)。传感器负责采集数据(网络包、系统日志等)、分析数据并生成安全事件。控制台主要起到中央管理的作用，商品化的产品通常提供图形界面的控制台，这些控制台基本上都支持 Windows NT 平台。入侵检测系统(intrusion detection system)采用的技术主要包括特征检测和异常检测两类。

1. 特征检测

特征检测(signature-based detection)技术将入侵活动定义为一种模式，入侵检测过程则是寻找与入侵行为相匹配的各种模式。该类技术能够很准确地将已有的入侵行为检查出来，但由于缺乏相匹配的模式，故无法检测到新的入侵行为。特征检测方式与计算机病毒扫描技术相类似，核心问题在于如何设计模式，尽可能地将各种非法活动囊括进来。

2. 异常检测

异常检测(abnormally detection)系统预先定义出一组正常运行的环境变量，主要包括 CPU 运行情况、内存利用率、网络平均流量等，这些环境信息可以人为地根据经验知识定义，也可以采用统计方法根据系统日常运行情况得出。当入侵检测系统在检测过程中发现运行数据与预先定义环境参数差异较大时，系统就会认定存在入侵情况，并进一步进行检查。这类技术的核心问题是如何准确地定义系统正常的环境变量。

2.3.2.2 常用入侵检测方法

据公安部计算机信息系统安全产品质量监督检验中心的报告，国内送检的入侵检测产品中 95%是属于使用入侵模板进行模式匹配的特征检测产品，少量是采用概率统计的统计检测产品与基于日志的专家知识库系统产品。入侵检测系统常用的检测方法有特征检测、统计检测与专家系统。

1. 特征检测

特征检测对已知的攻击或入侵的方式作出确定性的描述，形成相应的事件模式。当被审计的事件与已知的入侵事件模式相匹配时，即报警。该方法预报检测的准确率较高，但对于无经验知识的入侵与攻击行为无能为力。

2. 统计检测

在统计模型中常用的测量参数包括审计事件的数量、间隔时间、资源消耗情况等。常

用的入侵检测包括五种统计模型。

(1) 操作模型：该模型假设异常可通过测量结果与一些固定指标相比较得到，固定指标可以根据经验值或一段时间内的统计平均得到。

(2) 方差：计算参数的方差，设定其置信区间，当测量值超过置信区间的范围时表明有可能是异常。

(3) 多元模型：操作模型的扩展，通过同时分析多个参数实现检测。

(4) 马尔柯夫过程模型：将每种类型的事件定义为系统状态，用状态转移矩阵来表示状态的变化，状态矩阵的转移的概率较小则可能是异常事件。

(5) 时间序列分析：将事件计数与资源消耗用时间排成序列，如果一个新事件在该时间发生的概率较低，则该事件可能是入侵。

3. 专家系统

用专家系统对入侵进行检测，经常是针对特征入侵行为。专家系统的建立依赖于知识库的完备性，知识库的完备性又取决于审计记录的完备性与实时性。入侵的特征抽取与表达，是入侵检测专家系统的关键。专家系统防范的有效性完全取决于专家系统知识库的完备性。

2.3.3 重要入侵检测系统

按照检测对象划分，可以分为以下几种重要的入侵检测系统。

(1) 系统完整性检测(system integrity verifiers，SIV)：主要用于检测系统文件或注册表等重要位置信息是否被篡改，防止入侵者在入侵过程留下系统的后门。该类系统的工具软件较多，如"Tripwire"，它可以检测到重要系统组件的变动，但不产生实时报警信息。

(2) 网络入侵检测系统(network intrusion detection system，NIDS)：主要用于检测黑客或骇客通过网络进行的各类入侵行为。NIDS 的运用方式有两种，即在目标主机上以监测通信信息为主的检测模式，以及在独立机器上以监测网络设备运行为目标的单机模式。

(3) 日志文件监测器(log file monitors，LFM)：主要用于监测网络日志文件内容，这是一种特征检测技术的典型应用。LFM 通过将日志文件内容与关键字不断匹配，来获取入侵行为的存在。例如，对于 HTTP 服务器的日志文件，只要匹配"swatch"关键字，就能够检测到是否存在"PHF"攻击。

(4) 虚拟蜜网，也称为蜜罐系统(honeypots)：它是一个包含若干漏洞的诱骗系统。它通过模拟一个或多个易受到攻击的主机，为攻击者创造一个极易入侵的目标。由于每个蜜罐并无任何实际的运行活动，故任何接入都被认为是可以的。虚拟蜜网最大的优势在于它为真实的主机赢得了防范入侵的时间，拖延攻击者对真实目标的攻击；同时，诱捕系统能够不断获得攻击者的入侵行为，为真实目标制定有效的防护策略提供依据。

2.3.4 入侵检测发展方向

2.3.4.1 入侵技术的发展变化

入侵技术的发展与演化主要反映在下列几个方面：

(1) 入侵或攻击的综合化与复杂化。由于网络防范技术的多重化，攻击的难度增加，使得入侵者在实施入侵或攻击时往往同时采取多种入侵手段，以保证入侵的成功率，并可在攻击实施的初期掩盖攻击或入侵的真实目的。

(2) 入侵主体对象的间接化，即实施入侵与攻击的主体的隐蔽化。通过一定的技术，可掩盖攻击主体的源地址及主机位置。使用了隐蔽技术后，对于被攻击对象攻击的主体是无法直接确定的。

(3) 入侵或攻击的规模扩大。随着战争对电子技术与网络技术的依赖性逐步增强，其已逐步发展升级到电子战与信息战。对于信息战，无论其规模与技术，都不能与一般意义上的计算机网络的入侵与攻击相提并论。国家主干通信网络的安全与主权国家领土安全居于同等地位。

(4) 入侵或攻击技术的分布化。常用的入侵与攻击行为往往由单机执行。由于防范技术的发展使得此类行为不能奏效，所谓的分布式拒绝服务(DDoS)在很短时间内可造成被攻击主机的瘫痪。此类分布式攻击的信息模式与正常通信无差异，往往在攻击发动的初期不易被确认。分布式攻击是近期最常用的攻击手段。

(5) 攻击对象的转移。入侵与攻击常以网络为侵犯的主体，但近期的攻击行为却发生了策略性的改变，由攻击网络改为攻击网络的防护系统。现已有专门针对 IDS 作攻击的报道。攻击者详细地分析了 IDS 的审计方式、特征描述、通信模式，并针对 IDS 的弱点加以攻击。

2.3.4.2　入侵检测的发展方向

入侵检测技术的未来发展方向包括以下方面：

(1) 分布式入侵检测。一方面，针对分布式网络攻击的检测方法；另一方面，使用分布式的方法来检测网络攻击，涉及的关键技术为检测协同机制与入侵攻击的全局信息提取。

(2) 智能化入侵检测，即使用智能化的方法与手段来进行入侵检测。现阶段常用的智能算法有神经网络、遗传算法、模糊技术、免疫原理等方法，这些方法常用于入侵特征的辨识与泛化。利用专家系统的思想来构建入侵检测系统也是常用的方法之一。

(3) 全面的安全防御方案，即使用安全工程风险管理的思想与方法来处理网络安全问题，将网络安全作为一个整体工程来处理。从管理、网络结构、加密通道、防火墙、病毒防护、入侵检测多方位对所关注的网络作出评估，并提出可行的全面解决方案。

2.4　计算机病毒学

2.4.1　计算机病毒定义

计算机病毒(computer virus)在《中华人民共和国计算机信息系统安全保护条例》中被明确定义，病毒是指“编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。

计算机病毒往往会利用计算机操作系统的弱点进行传播，提高系统的安全性是防病

毒的一个重要方面，但过于强调提高系统的安全性将使系统多数时间用于病毒检查，使系统失去了可用性、实用性和易用性；另一方面，信息保密的要求让人们在泄密和防病毒之间无法选择。病毒与反病毒将作为一类对抗技术长期存在，两种技术都将随计算机技术的发展而得到长期的发展。

首先，应该明确病毒不是来源于突发或偶然的原因。一次突发的停电和偶然的错误，会在计算机的磁盘和内存中产生一些乱码和随机指令，但这些代码是无序和混乱的；病毒则是一种精巧严谨的代码，按照严格的秩序组织起来，与所在的系统网络环境相适应和配合起来，病毒不会通过偶然形成，并且需要有一定的长度，这个基本的长度从概率上来讲是不可能通过随机代码产生的。现在流行的病毒都是人为故意编写的，多数病毒可以找到作者和产地信息。从大量的统计分析来看，编写病毒的目的是：一些天才的程序员为了表现自己和证明自己的能力，出于对上司的不满，为了好奇，为了报复，为了祝贺和求爱，为了得到控制口令等，当然也有出于政治、军事、宗教、民族等方面的需求而专门编写的，其中也包括一些病毒研究机构和黑客的测试病毒。

2.4.1.1 病毒特征

计算机病毒具有以下几个特点：

(1) 寄生性。计算机病毒寄生在其他程序之中，当执行这个程序时，病毒就起破坏作用，而在未启动这个程序之前，它是不易被人发觉的。

(2) 传染性。计算机病毒不但本身具有破坏性，更具有传染性，一旦病毒被复制或产生变种，其速度之快令人难以预防。传染性是病毒的基本特征。计算机病毒会通过各种渠道从已被感染的计算机扩散到未被感染的计算机，在某些情况下造成被感染的计算机工作失常甚至瘫痪。是否具有传染性是判别一个程序是否为计算机病毒的最重要条件。病毒程序通过修改磁盘扇区信息或文件内容将自身嵌入到系统应用程序内部，被嵌入的程序叫做宿主程序。

(3) 潜伏性。有些病毒像定时炸弹一样，发作时间是预先设计好的。比如，黑色星期五病毒，不到预定时间无法觉察，当条件具备时，则会产生对系统的巨大破坏。潜伏性越好，其在系统中的存在时间就越长，病毒的传染范围就越大。潜伏性的第一种表现是指，病毒程序不用专用检测程序无法检查出来；潜伏性的第二种表现是指，计算机病毒的内部往往有一种触发机制，不满足触发条件时，计算机病毒除了传染外不做任何破坏。

(4) 隐蔽性。计算机病毒具有很强的隐蔽性，有的可以通过病毒软件检查出来，有的根本就查不出来，这类病毒处理起来通常很困难。

(5) 破坏性。计算机中毒后，会导致正常的程序无法运行，删除或破坏计算机内的文件。

2.4.1.2 病毒命名

病毒命名的一般格式为：

＜病毒前缀＞.＜病毒名＞.＜病毒后缀＞

病毒前缀是指一个病毒的种类，用来区别病毒的种族。不同种类的病毒，其前缀也是

不同的。比如，常见的木马病毒的前缀是 Trojan，蠕虫病毒的前缀是 Worm 等。

病毒名是指一个病毒的家族特征，用来区别和标识病毒家族。比如，著名的 CIH 病毒的家族名都是统一的“CIH”，振荡波蠕虫病毒的家族名是“Sasser”。

病毒后缀是指一个病毒的变种特征，用来区别具体某个家族病毒的变种，一般都采用英文中的 26 个字母来表示。比如，Worm. Sasser. b 是指振荡波蠕虫病毒的变种 B，一般称为“振荡波 B 变种”或者“振荡波变种 B”。

病毒的主名称是由分析员根据病毒体的特征字符串、特定行为或者所使用的编译平台来定的，如果无法确定则可以用字符串“Agent”来代替主名称，小于 10KB 大小的文件可以命名为“Small”。

版本信息只允许为数字，对于版本信息不明确的不加版本信息。

如果病毒的主行为类型、行为类型、宿主文件类型、主名称均相同，则认为是同一家族的病毒，这时要用变种号来区分不同的病毒记录。如果一位版本号不够用则最多可以扩展 3 位，并且均为小写字母 a～z，如 aa、ab、aaa、aab，依此类推。病毒的版本号码由系统自动计算，不需要人工输入或选择。

2.4.2 计算机病毒分类

1. 按照计算机病毒存在的媒体进行分类

按照计算机病毒存在的媒体，病毒可分为网络病毒、文件病毒、引导型病毒。网络病毒通过计算机网络传播感染网络中的可执行文件；文件病毒感染计算机中的文件（如 COM、EXE、DOC 等）；引导型病毒感染启动扇区（Boot）和硬盘的系统引导扇区（MBR）。还有这三种情况的混合型，例如，多型病毒（文件和引导型）感染文件和引导扇区两种目标，这样的病毒通常都具有复杂的算法，它们使用非常规的办法侵入系统，同时使用了加密和变形算法。

2. 按照计算机病毒传染的方法进行分类

按照计算机病毒传染的方法，病毒可分为驻留型病毒和非驻留型病毒。驻留型病毒感染计算机后，把自身的驻留部分放在内存（RAM）中，这一部分程序挂接系统并合并到操作系统中去，处于激活状态；非驻留型病毒在得到机会激活时并不感染计算机内存。

3. 按照病毒破坏的能力进行分类

（1）无害型：除了传染时减少磁盘的可用空间外，对系统没有其他影响。

（2）无危险型：这类病毒仅仅是减少内存、显示图像、发出声音。

（3）危险型：这类病毒在计算机系统操作中造成严重的错误。

（4）非常危险型：这类病毒删除程序、破坏数据、清除系统内存区和操作系统中重要的信息，由病毒引起的其他程序产生的错误也会破坏文件和扇区。

4. 按照病毒特有的算法进行分类

（1）伴随型病毒：这一类病毒并不改变文件本身，它们根据算法产生 EXE 文件的伴随体，具有同样的名字和不同的扩展名（COM），例如，XCOPY. EXE 的伴随体是 XCOPY. COM。病毒把自身写入 COM 文件并不改变 EXE 文件，当 DOS 加载文件时，伴随体优先被执行，再由伴随体加载执行原来的 EXE 文件。

(2)“蠕虫”型病毒：通过计算机网络传播，不改变文件和资料信息，利用网络从一台机器的内存传播到其他机器的内存中，计算网络地址，将自身的病毒通过网络发送。

(3)寄生型病毒：除了伴随和“蠕虫”型，其他病毒均可称为寄生型病毒，它们依附在系统的引导扇区或文件中，通过系统的功能进行传播。

(4)诡秘型病毒：它们一般不直接修改DOS中断和扇区数据，而是通过文件缓冲区进行DOS内部修改，利用DOS空闲的数据区进行工作。

(5)变型病毒(又称幽灵病毒)：这一类病毒使用复杂的算法，使自己每传播一份都具有不同的内容和长度。变型病毒一般由一段混有无关指令的解码算法和被变化过的病毒体组成。

5. 按照病毒的攻击目标进行分类

(1)DOS病毒：针对DOS操作系统开发的病毒。由于Windows 9x病毒的出现，DOS病毒几乎绝迹。但DOS病毒在Windows 9x环境中仍可以进行感染活动，因此若执行染毒文件，Windows 9x用户的系统也会被感染。

(2)Windows病毒：针对Windows 9x操作系统的病毒。现在的计算机用户一般都安装Windows系统，其中最典型的病毒有CIH病毒。一些Windows病毒不仅在Windows 9x上正常感染，还可以感染Windows NT上的其他文件。

(3)其他系统病毒：主要攻击Linux、UNIX、OS2及嵌入式系统的病毒。由于系统本身的复杂性，这类病毒数量不是很多。

6. 根据链接方式进行分类

(1)源码型病毒：该病毒攻击高级语言编写的程序，在高级语言所编写的程序编译前插入源程序中，经编译成为合法程序的一部分。

(2)嵌入型病毒：这种病毒是将自身嵌入到现有程序中，把计算机病毒的主体程序与其攻击的对象以插入的方式链接。这种计算机病毒是难以编写的，一旦侵入程序体后也较难消除。如果同时采用多态性病毒技术、超级病毒技术和隐蔽性病毒技术，将给当前的反病毒技术带来严峻的挑战。

(3)外壳型病毒：外壳型病毒将其自身包围在主程序的四周，对原来的程序不作修改。这种病毒最为常见，易于编写，也易于发现，一般测试文件的大小即可察觉。

(4)操作系统型病毒：这种病毒用自身的程序加入或取代部分操作系统进行工作，具有很强的破坏力，可以导致整个系统的瘫痪。圆点病毒和大麻病毒就是典型的操作系统型病毒。

2.4.3 病毒危害与防范

1983年11月3日，Fred Cohen博士研制出一种在运行过程中可以复制自身的破坏性程序。Len Adleman将这种破坏性程序命名为计算机病毒，并在每周一次的计算机安全讨论会上正式提出，8小时后专家们在VAX11/750计算机系统上成功运行该程序，这样，第一个病毒实验成功。

计算机病毒之所以称为病毒，是因为其具有传染的本质。传染渠道通常有以下几种：

(1)通过介质。由于使用带有病毒的介质，使机器感染病毒发病，并传染给未被感

染的“干净”的移动介质。大量的数据交换，合法或非法的程序复制，加速病毒感染。

（2）通过硬盘。通过硬盘传染也是重要的渠道，由于带有病毒的机器移到其他地方使用、维修等，使病毒发生扩散。

（3）通过网络。这种传染扩散极快，能在很短的时间内传遍整个网络。通过网络传染病毒有两种途经：一种是文件下载，这些被浏览的或是被下载的文件可能存在病毒；另一种是电子邮件，大多数邮件系统提供了在网络间传送附带格式化文档邮件的功能，网络使用的简易性和开放性使得这种威胁越来越严重。

2.4.3.1 计算机病毒危害

世界上已出现的最著名的计算机病毒包括以下几类。

1. Elk Cloner（1982 年）

它被看做攻击个人计算机的第一款全球病毒。它通过苹果 Apple Ⅱ软盘进行传播。这个病毒被放在一个游戏磁盘上，可以被使用 49 次。在第 50 次使用的时候，它并不运行游戏，取而代之的是打开一个空白屏幕，并显示一首短诗。

2. Brain（1986 年）

Brain 是第一款攻击 DOS 操作系统的病毒，可以感染软盘，该病毒会填充满软盘上未用的空间，而导致它不能再被使用。

3. Morris（1988 年）

该病毒程序利用了系统存在的弱点进行入侵，Morris 设计的最初目的并不是搞破坏，而是用来测量网络的大小。但是，由于程序的循环没有处理好，计算机会不停地执行，最终导致死机。

4. CIH（1998 年）

CIH 病毒是迄今为止破坏性最严重的病毒，也是世界上首例破坏硬件的病毒。它发作时不仅破坏硬盘的引导区和分区表，而且破坏计算机系统 BIOS，导致主板损坏。此病毒是由台湾大学生陈盈豪研制的。

5. Melissa（1999 年）

Melissa 是最早通过电子邮件传播的病毒之一，当用户打开一封电子邮件的附件，病毒会自动发送到用户通讯簿中的前 50 个地址，因此这个病毒在数小时之内传遍全球。

6. Love bug（2000 年）

Love bug 也是通过电子邮件附件进行传播，把病毒伪装成一封求爱信来欺骗收件人打开。这个病毒以其传播速度和范围让安全专家吃惊。在数小时之内，这个小小的计算机程序征服了全世界范围之内的计算机系统。

7. 红色代码（2001 年）

红色代码被认为是史上最昂贵的计算机病毒之一，这个自我复制的恶意病毒利用了微软 IIS 服务器中的一个漏洞。该蠕虫病毒具有一个更恶毒的版本，被称做红色代码Ⅱ，被感染的系统性能会严重下降。

8. Nimda（2001 年）

尼姆达（Nimda）是历史上传播速度最快的病毒之一，在上线之后的 22 分钟之后就成为传播最广的病毒。

9．冲击波(2003 年)

冲击波病毒的英文名称是 Blaster，还被叫做 Lovsan 或 Lovesan，它利用了微软软件中的一个缺陷，对系统端口进行疯狂攻击，可以导致系统崩溃。

10．震荡波(2004 年)

震荡波是又一个利用 Windows 缺陷的蠕虫病毒，可以导致计算机崩溃并不断重启。

11．熊猫烧香(2007 年)

熊猫烧香会使所有程序图标变成熊猫烧香，并使它们不能应用。

12．扫荡波(2008 年)

扫荡波也是个利用漏洞从网络入侵的程序。大批用户关闭自动更新以后，加剧了这个病毒的蔓延，可以导致被攻击者的机器被完全控制。

13．木马下载器(2009 年)

此病毒会产生 1000～2000 个不等的木马病毒，导致系统崩溃。

14．鬼影病毒(2010 年)

该病毒成功运行后，在进程中、系统启动加载项里找不到任何异常，同时即使格式化重装系统，也无法彻底清除该病毒。

表 2.1 显示了近年来几个病毒带来的巨大危害。

表 2.1　重大病毒危害列表

年份	攻击行为发起者	受害 PC 数目	损失金额(美元)
2006	木马和恶意软件	(破坏程度不可估计)	(破坏程度不可估计)
2005	木马	(破坏程度不可估计)	(破坏程度不可估计)
2004	Worm_Sasser(震荡波)	(破坏程度不可估计)	(破坏程度不可估计)
2003	Worm_MSBLAST(冲击波)	超过 140 万台	(破坏程度不可估计)
2003	SQL Slammer	超过 20 万台	9.5 亿～12 亿
2002	Klez	超过 600 万台	90 亿
2001	RedCode	超过 100 万台	26 亿
2001	NIMDA	超过 800 万台	60 亿
2000	Love Letter	(破坏程度不可估计)	88 亿
1999	CIH	超过 6000 万台	近 100 亿

2.4.3.2　反病毒技术

从反病毒产品对计算机病毒的作用来讲，反病毒技术可以分为病毒预防技术、病毒检测技术及病毒清除技术。

1．病毒预防技术

计算机病毒的预防技术就是通过一定的技术手段防止计算机病毒对系统的传染和破坏，是一种行为规则判定技术。具体来说，计算机病毒的预防是通过阻止计算机病毒进入系统内存或阻止计算机病毒对磁盘的操作，尤其是写操作。

病毒预防技术包括磁盘引导区保护、加密可执行程序、读写控制技术、系统监控技术等。计算机病毒的预防应用包括对已知病毒的预防和对未知病毒的预防两个部分。目前,对已知病毒的预防可以采用特征判定技术或静态判定技术;而对未知病毒的预防则是一种行为规则的判定技术,即动态判定技术。

2. 病毒检测技术

计算机病毒的检测技术是指通过一定的技术手段判定出特定计算机病毒的一种技术。它有两种:一种是根据计算机病毒的关键字、特征程序段内容、病毒特征及传染方式、文件长度的变化,在特征分类的基础上建立的病毒检测技术;另一种是不针对具体病毒程序的自身校验技术,即对某个文件或数据段进行检验和计算并保存其结果,以后定期或不定期地以保存的结果对该文件或数据段进行检验,若出现差异,即表示该文件或数据段的完整性已遭到破坏,感染上了病毒,从而检测到病毒的存在。

3. 病毒清除技术

计算机病毒的清除技术是计算机病毒检测技术发展的必然结果,是计算机病毒传染程序的一种逆过程。目前,清除病毒大都是在某种病毒出现后,通过对其进行分析研究而研制出具有相应解毒功能的软件。这类软件技术发展往往是被动的,带有滞后性。由于计算机软件所要求的精确性,解毒软件有其局限性,对变种病毒的清除无能为力。

2.4.4 防护与检测策略

在网络环境下,防范病毒问题显得尤其重要,因此,采用高效的网络防病毒方法和技术是一件非常重要的事情。

2.4.4.1 病毒防护技术

网络病毒防护有以下四种基本方法。

1. 基于网络目录和文件安全性方法

网络上公用目录或共享目录的安全性防范措施,对于防止病毒在网上传播起到积极作用。至于网络用户的私人目录,由于其限于个别使用,病毒很难传播给其他用户。采用基于网络目录和文件安全性的方法对防止病毒起到了一定作用,但是这种方法毕竟是基于网络操作系统的安全性的设计,存在着局限性。

2. 采用工作站防病毒芯片

这种方法是将防病毒功能集成在一个芯片上,安装在网络工作站上,以便经常性地保护工作站及其通往服务器的路径。芯片具备工作站存取控制与病毒保护能力,芯片插在网卡的 EPROM 槽内,可以令用户免除许多烦琐的管理工作。

3. 采用 Station Lock 网络防毒方法

Station Lock 是著名防病毒产品开发商 Trend Micro Devices 公司的新一代网络防病毒产品。其防毒概念是建立在“病毒必须执行有限数量的程序之后,才会产生感染效力”的基础之上。引导型病毒必须使用系统的 BIOS 功能调用;文件型病毒必须将自己所有的程序代码复制到另一个系统执行文件时才能复制感染;混合型病毒和多形体病毒在实施感染之前也必须获取系统控制权,才能运行病毒体程序而实施感染。Station Lock 就是通过这些特点,用间接方法观察,精确地预测病毒的攻击行为。其作用对象包括多型

体病毒和未来型病毒。

4. 基于服务器的防毒技术

服务器是网络的核心，一旦服务器被病毒感染，就会使服务器无法启动，整个网络陷于瘫痪，造成灾难性后果。目前，基于服务器的防治病毒方法大都采用了 NLM(NetWare load module)技术，以 NLM 模块方式进行程序设计，以服务器为基础，提供实时扫描病毒能力。市场上的产品，如 Central Point 公司的 AntiVirus for Networks、Intel 公司的 LANdesk Virus Protect 以及南京威尔德计算机公司的 LANclear for NetWare 等都是采用以服务器为基础的防病毒技术。这些产品的目的都是保护服务器，使服务器不被感染。这样，病毒也就失去了传播途径，因而从根本上杜绝了病毒在网上蔓延。

在上述四种网络防毒技术中，Station Lock 是一种针对病毒行为的防治方法，Station Lock 目前已能提供 Intel 以太网络接口卡支持，而且未来还将支持各种普及型的以太令牌环(Token-Ring)网络接口卡。基于服务器的防治病毒方法，表现在可以集中式扫毒，能实现实时扫描功能，软件升级方便。特别是当联网的机器很多时，利用这种方法比为每台工作站都安装防病毒产品要节省成本。其代表性的产品有 LANdesk、LANClear for NetWare 等。

5. 实时反病毒技术

实时反病毒技术一向为反病毒界所看好，被认为是比较彻底的反病毒解决方案。多年来其发展之所以受到制约，一方面是因为它需要占用一部分系统资源而降低系统性能；另一方面是因为它与其他软件(特别是操作系统)的兼容性问题始终没有得到很好的解决。

随着硬件处理速度的不断提高，实时化反病毒技术所造成的系统负荷已经降低到了可被大家忽略的程度，而 Windows 操作系统的多任务、多线程环境，又为实时反病毒技术提供了良好的运行环境。实时反病毒技术重新得到重视。

2.4.4.2 病毒检测技术

1. 比较法

比较法是用原始备份与被检测的引导扇区或被检测的文件进行比较。比较时可以靠打印的代码清单(比如 Debug 的 D 命令输出格式)进行比较，或用程序来进行比较(如 DOS 的 Diskcomp、FC 或 PCTools 等其他软件)。这种比较法不需要专用的计算机病毒检测程序，只要用常规 DOS 软件和 PCTools 等工具软件就可以进行。而且用这种比较法还可以发现那些尚不能被现有的计算机病毒查毒程序发现的计算机病毒。通过代码分析，可以判定某个程序中是否含有计算机病毒，发现新计算机病毒就必须依靠比较法和分析法一同工作。

比较法的优点是简单、方便，无需专用软件；缺点是无法确认计算机病毒的种类名称。另外，造成被检测程序与原始备份之间差别的原因尚需进一步验证，以查明是由于计算机病毒造成的，还是由于 DOS 数据被偶然原因，如突然停电、程序失控、恶意程序等破坏的。另外，当找不到原始备份时，用比较法就不能马上得到结论。

2. 加总比对法

根据每个程序的档案名称、大小、时间、日期及内容，加总为一个检查码，再将检查码

附于程序的后面，或是将所有检查码放在同一个数据库中，再利用加总比对系统，追踪并记录每个程序的检查码是否遭更改，以判断是否感染了计算机病毒。

这种技术可侦测到各式的计算机病毒，但最大的缺点就是误判率高，且无法确认是哪种计算机病毒感染的。此外，对于隐形计算机病毒无法侦测到。

3. 搜索法

搜索法是用每一种计算机病毒体含有的特定字符串对被检测的对象进行扫描。如果在被检测对象内部发现了某一种特定字节串，就表明发现了该字节串所代表的计算机病毒。国外将这种按搜索法工作的计算机病毒扫描软件称为 Virus Scanner。计算机病毒扫描软件由两部分组成：一部分是计算机病毒代码库，含有经过特别选定的各种计算机病毒的代码串；另一部分是利用该代码库进行扫描的扫描程序。目前常见的防杀计算机病毒软件对已知计算机病毒的检测大多采用这种方法。计算机病毒扫描程序能识别的计算机病毒的数目完全取决于计算机病毒代码库内所含计算机病毒的种类多少。显而易见，库中计算机病毒代码种类越多，扫描程序能认出的计算机病毒就越多。

这种扫描法的缺点也是明显的，具体如下：

(1) 当被扫描的文件很长时，扫描所花时间也较多。

(2) 新的计算机病毒的特征串未加入计算机病毒代码库时，老版本的扫毒程序无法识别出新的计算机病毒。

(3) 怀有恶意的计算机病毒制造者得到代码库后，会很容易地改变计算机病毒体内的代码，生成一个新的变种，使扫描程序失去检测它的能力。

(4) 容易产生误报。

(5) 不易识别多维变形计算机病毒。

4. 分析法

分析法常为计算机病毒技术人员使用。使用分析法的目的在于：

(1) 确认被观察的磁盘引导扇区和程序中是否含有计算机病毒。

(2) 确认计算机病毒的类型，判定其是否是一种新的计算机病毒。

(3) 搞清楚计算机病毒体的大致结构，提取特征识别用的字节串或特征字，用于增添到计算机病毒代码库供计算机病毒扫描和识别程序用。

(4) 详细分析计算机病毒代码，制定相应的防杀计算机病毒方案。

使用分析法要求具有比较全面的有关计算机、DOS、Windows、网络等的结构和功能调用以及关于计算机病毒方面的各种知识，这是与其他检测计算机病毒方法不一样的地方。

除了要具有相关的知识外，还需要反汇编工具、二进制文件编辑器等分析用工具程序和专用的试验计算机。计算机病毒检测的分析法是防杀计算机病毒工作中不可缺少的重要技术，任何一个性能优良的防杀计算机病毒系统的研制和开发都离不开专门人员对各种计算机病毒的详尽而认真的分析。

分析的步骤分为静态分析和动态分析两种。静态分析是指利用反汇编工具将计算机病毒代码打印成反汇编指令清单后进行分析。分析人员具有的素质越高，分析过程越快，理解越深。动态分析则是指利用 Debug 等调试工具在内存带毒的情况下，对计算机病毒

做动态跟踪，观察计算机病毒的具体工作过程，以进一步在静态分析的基础上理解计算机病毒工作的原理。

5. 人工智能陷阱技术和宏病毒陷阱技术

人工智能陷阱是一种监测计算机行为的常驻式扫描技术。它将所有计算机病毒所产生的行为归纳起来，一旦发现内存中的程序有任何不当的行为，系统就会有所警觉，并告知使用者。这种技术的优点是执行速度快、操作简便，且可以侦测到各式计算机病毒；缺点是程序设计难，且不容易考虑周全。

宏病毒陷阱技术（MacroTrap）是结合了搜索法和人工智能陷阱技术，依行为模式来侦测已知及未知的宏病毒。其中，配合 OLE2 技术，可将宏与文件分开，使得扫描速度变得飞快，而且更可有效地将宏病毒彻底清除。

6. 软件仿真扫描法

该技术专门用来对付多态变形计算机病毒（polymorphic/mutation virus）。多态变形计算机病毒在每次传染时，都将自身以不同的随机数加密于每个感染的文件中，传统搜索法的方式根本就无法找到这种计算机病毒。软件仿真技术则是成功地仿真 CPU 执行，在 DOS 虚拟机（virtual machine）下伪执行计算机病毒程序，安全并准确地将其解密，再加以扫描。

7. 先知扫描法

先知扫描技术（virus instruction code emulation，VICE）是继软件仿真后的一大技术上的突破。先知扫描技术将专业人员用来判断程序是否存在计算机病毒代码的方法，分析归纳成专家系统和知识库，再利用软件模拟技术（software emulation）伪执行新的计算机病毒，超前分析出新计算机病毒代码，防范后续的计算机病毒。

2.5 网络安全管理规范

信息网络运行部门的安全管理工作应首先研究确定网络安全策略，即网络安全保护工作的目标和对象。网络安全策略包括总体安全策略、应用系统安全策略、部门安全策略、设备安全策略等。

2.5.1 信息网络安全策略

信息网络总体安全策略可以概括为“实体可信，行为可控，资源可管，事件可查，运行可靠”，总体安全策略为其他安全策略的制定提供总的依据。

1. 实体可信

实体指构成信息网络的基本要素，主要有网络基础设备、软件系统、用户和数据。实体可信就是保证构建网络的基础设备和软件系统安全可信，没有预留后门；保证接入网络的用户是可信的，防止恶意用户对系统的攻击破坏；保证在网络上传输、处理、存储的数据是可信的，防止搭线窃听、非授权访问或恶意篡改。

2. 行为可控

保证用户行为可控，即保证本地计算机的各种软硬件资源不被非授权使用或被用于

危害本系统或其他系统的安全；保证网络接入可控，即保证用户接入网络应严格受控，用户上网必须得到许可；保证网络行为可控，即保证网络上的通信行为受到监视和控制，防止滥用资源、非法外联、网络攻击、非法访问和传播有害信息等恶意事件的发生。

3. 资源可管

保证对路由器、交换机、服务器、邮件系统、数据库、域名系统、安全设备、密码设备、交换机端口、IP 地址、用户账号、服务端口等网络资源进行统一管理。

4. 事件可查

保证对网络上的各类违规事件进行监控记录，确保日志记录的完整性，为安全事件稽查、取证提供依据。

5. 运行可靠

保证网络在发生自然灾难或遭到硬摧毁时仍能不间断运行，具有容灾抗毁和备份恢复能力；保证能够有效防范病毒和黑客的攻击所引起的网络拥塞、系统崩溃和数据丢失，具有较强的应急响应和灾难恢复能力。

2.5.2 信息网络管理机制

信息网络安全管理坚持“谁主管谁负责，谁运行谁负责”的原则。

信息安全管理组织的主要职责是：制定工作人员守则、安全操作规范和管理制度，经主管领导批准后监督执行；组织进行信息网络建设和运行安全检测检查，掌握详细的安全资料，研究制定安全对策和措施；负责信息网络的日常安全管理工作；定期总结安全工作，并接受公安机关公共信息网络安全监察部门的工作指导。

信息网络安全管理的主要内容：由主要领导负责的逐级安全保护管理责任制，配备专职或兼职的安全员，各级职责划分明确，并有效开展工作；明确运行和使用部门的岗位责任制，建立安全管理规章制度；在职工群众中普及安全知识，对重点岗位职工进行专门培训和考核；采取必要的安全技术措施；对安全保护工作有档案记录和应急计划；定期进行安全检测、风险分析和安全隐患整改；实行信息安全等级保护制度。

信息网络安全管理工作要坚持从实际出发、保障重点的原则，区分不同情况，分级、分类、分阶段进行信息网络安全建设和管理。按照《计算机信息系统安全保护等级划分准则》的规定，我国实行五级信息安全等级保护。

第一级：用户自主保护级。由用户来决定如何对资源进行保护，以及采用何种方式进行保护。

第二级：系统审计保护级。本级的安全保护机制支持用户具有更强的自主保护能力，特别是具有访问审记能力，即它能创建、维护受保护对象的访问审计跟踪记录，记录与系统安全相关的事件发生的日期、时间、用户和事件类型等信息，所有和该事件相关的操作都能够被记录下来，以便当系统发生安全问题时，可以根据审计记录，分析追查事故责任人。

第三级：安全标记保护级。具有第二级系统审计保护级的所有功能，并对访问者及其访问对象实施强制访问控制。通过对访问者和访问对象指定不同安全标记，限制访问者的权限。

第四级：结构化保护级。将前三级的安全保护能力扩展到所有访问者和访问对象，支持形式化的安全保护策略。其本身构造也是结构化的，以使之具有相当的抗渗透能力。本级的安全保护机制能够使信息系统实施一种系统化的安全保护。

第五级：访问验证保护级。具备第四级的所有功能，还具有仲裁访问者能否访问某些对象的能力。为此，本级的安全保护机制不能被攻击、被篡改，具有极强的抗渗透能力。

计算机信息系统安全等级保护标准体系包括信息系统安全保护等级划分标准、等级设备标准、等级建设标准、等级管理标准等，是实行等级保护制度的重要基础。

2.5.3 安全事件响应机制

从用户的角度看，安全事件包括个人隐私或商业利益的信息在网络上受到侵犯，其他人或竞争对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私，破坏信息的机密性、完整性和真实性。

从网络运行和管理者角度来看，安全事件是对本地网络信息的访问、读写等操作，出现病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，或遭受网络黑客的攻击。

从保密部门来看，安全事件则是国家重要信息泄露，对社会产生危害，对国家造成巨大损失。

从社会教育和意识形态角度来看，在网络上传播不健康的内容，对社会稳定和人类发展造成阻碍等都是安全事件。

从网络运行和管理来看，安全事件的响应处置包括六个阶段。

(1) 准备阶段：基于威胁建立一组合理的防范、控制措施，建立一组尽可能高效的事件处理程序，获得处理问题必需的资源和人员，最终建立应急响应体系。

(2) 检测阶段：进行技术检测，获取完整的系统备份，进行系统审计，分析异常现象，评估事件范围，报告事件。

(3) 控制阶段：制定可能的控制策略，拟定详细的控制措施实施计划，对控制措施进行评估和选择，记录控制措施的执行。

(4) 根除阶段：查找出事件根源并根除，确认备份系统的安全，记录和报告。

(5) 恢复阶段：根据事件情况，从保存完好的介质上恢复系统，一次完整的恢复应包括修改所有用户口令。

(6) 追踪阶段：回顾并整合发生事件，对事件进行一次事后分析，为下一步进行的民事或刑事的法律活动提供有用的信息。

第 3 章　网络分析实验

3.1　网络分析原理

3.1.1　TCP/IP 原理

TCP/IP 是一个四层协议系统，TCP/IP 协议族是一组不同的协议组合在一起构成的协议族。

数据发送时自上而下，层层加码；数据接收时自下而上，层层解码。

如图 3.1 所示，当应用程序用 TCP 传送数据时，数据被送入协议栈中，然后逐层通过直到被当做一串比特流送入网络。每一层对收到的数据都要增加一些首部信息(有时还要增加尾部信息)。TCP 传给 IP 的数据单元称做 TCP 报文段。IP 传给网络接口层的数据单元称做 IP 数据报。通过以太网传输的比特流称做帧。

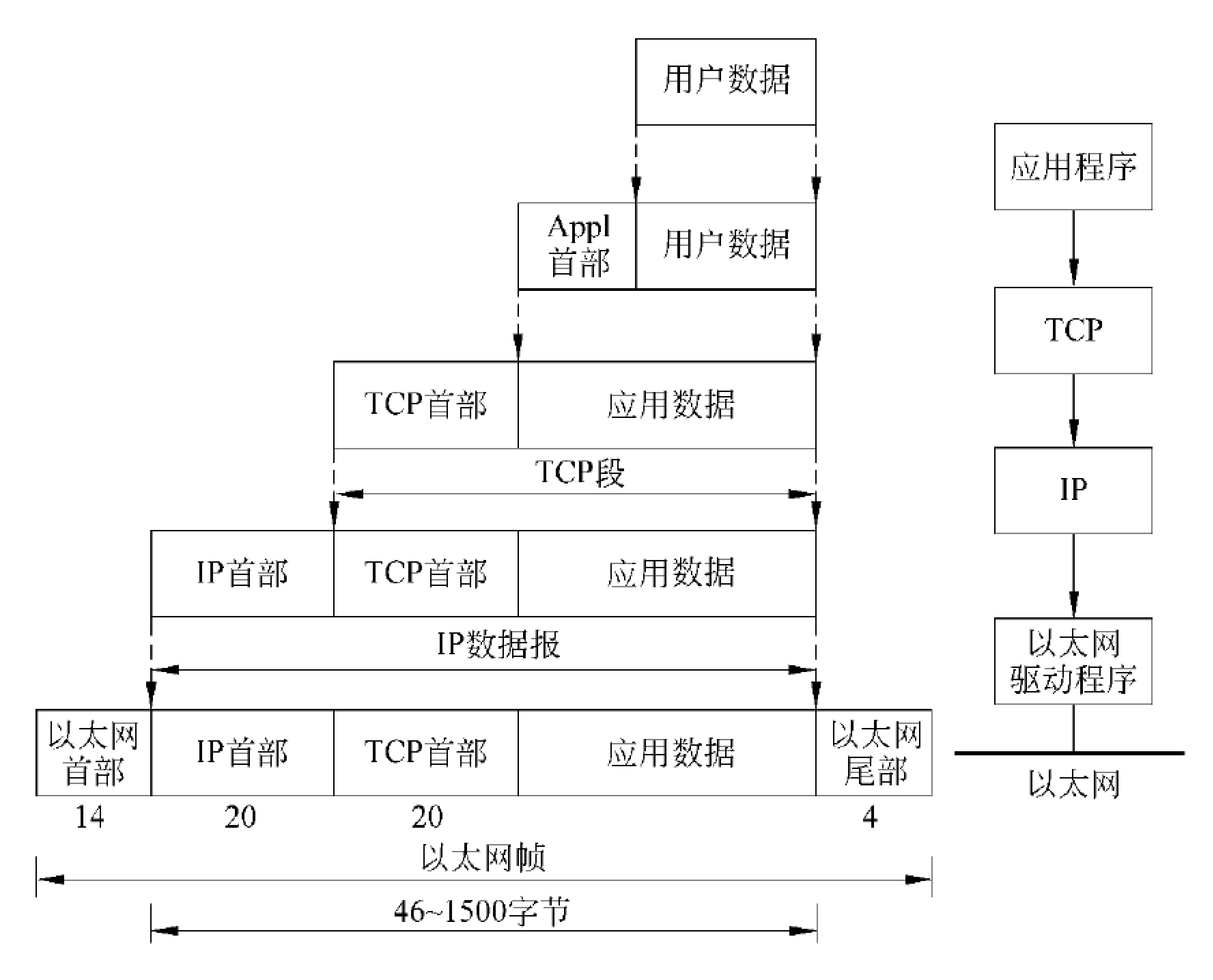


图 3.1　TCP/IP 协议系统

垂直方向是当今普遍认可的数据处理的功能流程。每一层都有与其相邻层的接口。为了通信，系统必须在各层之间传递数据、指令、地址等信息，通信的逻辑流程与真正的数据流不同，虽然通信流程垂直通过各层次，但每一层都在逻辑上与远程计算机系统的相应协议层直接通信。如图 3.2 所示，通信实际上是按垂直方向进行的，但在逻辑上通信是在同层进行的。

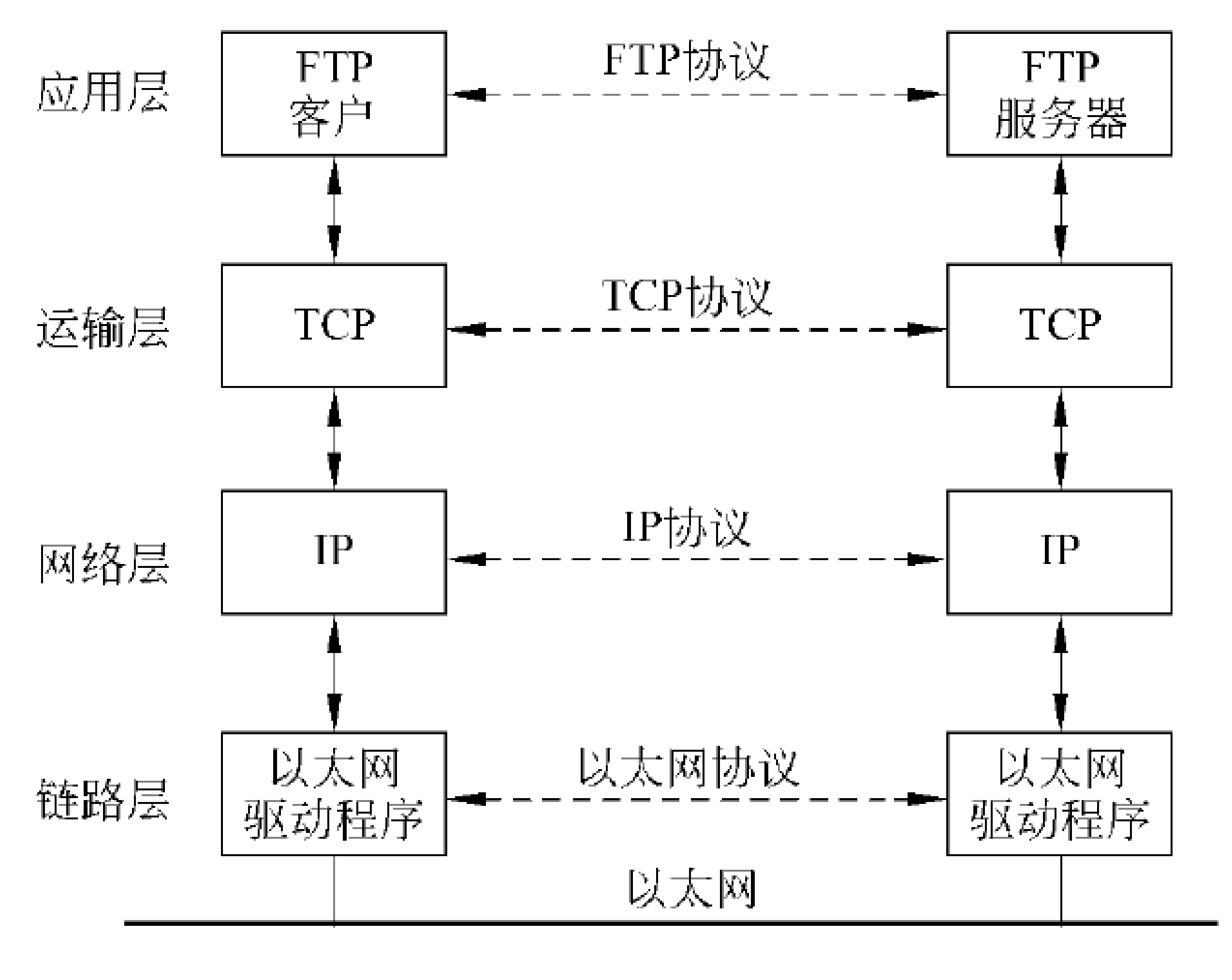


图 32　逻辑通信结构

3.1.2　交换技术

所谓交换，就是将分组（或帧）从一个端口转移到另一端口的动作。交换机在操作过程中不断地收集资料去建立它本身的一个地址表，MAC 地址表显示了主机的 MAC 地址与以太网交换机端口的映射关系，指出数据帧去往的目标主机。

当以太网交换机收到一个数据帧时，将数据帧的目的 MAC 地址与 MAC 地址表进行查找匹配。如果在 MAC 地址表中没有相应的匹配项，则向除接收端口外的所有端口广播该数据帧。当 MAC 地址表中有匹配项时，该匹配项指定的交换机端口与接收端口相同则表明该数据帧的目的主机和源主机在同一广播域中，不通过交换机也可以完成通信，交换机将丢弃该数据帧。否则，交换机把该数据帧转发到相应的端口。

交换机检查收到数据帧的源 MAC 地址，并查找 MAC 地址表中与之相匹配的项。如果没有，交换机将记录该 MAC 地址和接收该数据帧的端口，并激活一个定时器。这个过程被称做地址学习；而如果接收的数据帧的源 MAC 地址在地址表中有匹配项，交换机将复位该地址的定时器。如果交换机不能正确学习 MAC 地址，则有可能造成数据包丢失以及泛洪现象的发生，影响交换机的转发性能。

局域网交换技术是作为对共享式局域网提供有效的网段划分的解决方案，可以使用户尽可能地分享到最大带宽。交换技术在 OSI 七层网络模型中的第二层，即数据链路层进行操作，交换机对数据包的转发建立在 MAC 地址基础上，对于 IP 网络协议来说，它是透明的，即交换机在转发数据包时，无须知道信源机和目标机的 IP 地址，只须知道其物理地址。

3.1.3　路由技术

路由是指通过相互联接的网络把信息从源地点移动到目标地点的过程。在路由过程中，信息至少会经过一个或多个中间节点。路由和交换所实现的功能类似，但二者的区别是明显的：交换发生在 OSI 参考模型的第二层（数据链路层），而路由发生在第三层，即网

络层。这一区别决定了路由和交换在传输信息的过程中需要使用不同的控制信息。

当 IP 子网中的一台主机发送 IP 分组给同一子网的另一台主机时，它将直接把 IP 分组送到网络上，对方就能收到。当发送给不同子网上的主机时，它要选择一个能到达目的子网上的路由器，把 IP 分组传递给该路由器，由路由器负责把 IP 分组送到目的地。如果没有这样的路由器，主机就把 IP 分组送给一个被称为“默认网关”的路由器。“默认网关”是每台主机上的一个配置参数，它是同一个网络上的某个路由器端口的 IP 地址。

同主机一样，路由器也要判定端口连接的是否为目的子网，如果是，就直接把分组通过端口送到网络上，否则，也要选择下一个路由器来传送分组。路由器也有它的默认网关，用来传送 IP 分组，通过逐级传送，IP 分组最终将送到目的地，否则 IP 分组被网络丢弃。

路由器不仅负责 IP 分组转发，还需与其他路由器联络，确定网络的路由选择和维护路由表。路由包含两个基本的动作：选择最佳路径和通过网络传输信息。在路由过程中，后者也称为(数据)交换。交换相对来说比较简单，而选择路径很复杂。

路径选择是判定到达目的地的最佳路径，由路由选择算法来实现。由于涉及不同的路由选择协议和路由选择算法，要相对复杂一些。为了判定最佳路径，路由选择算法必须启动并维护包含路由信息的路由表，其中路由信息依赖于所用的路由选择算法。

Metric 是路由算法用以确定到达目的地的最佳路径的计量标准。路由算法根据许多信息来填充路由表。路由器查看了数据包的目的协议地址后，确定是否知道如何转发该包。如果路由器不知道如何转发，通常就将之丢弃。如果路由器知道如何转发，就把目的物理地址变成下一跳的物理地址并向之发送。下一跳可能就是最终的目的主机，如果不是，通常为另一个路由器，它将执行同样的步骤。

3.1.4 网络嗅探技术

3.1.4.1 嗅探技术简介

嗅探(sniffer)技术是一种重要的网络安全攻防技术。对黑客来说，通过嗅探技术能以非常隐蔽的方式攫取网络中的大量敏感信息。与主动扫描相比，嗅探行为更难被察觉，也更容易操作。对安全管理人员来说，借助嗅探技术，可以对网络活动进行实时监控，发现各种网络攻击行为。嗅探技术最初是作为网络管理员检测网络通信的必备技术，既可以是软件，又可以是一个硬件设备。软件 Sniffer 应用方便，针对不同的操作系统平台都有多种不同的软件 Sniffer；硬件 Sniffer 通常被称做协议分析器，其价格一般都很高昂。

在局域网中，由于以太网的共享特性决定了嗅探能够成功。因为以太网是基于广播方式传送数据的，所有的物理信号都会被传送到每一个主机节点，此外，网卡可以被设置成混杂接收模式，在这种模式下，无论监听到的数据帧目的地址如何，网卡都能予以接收。而 TCP/IP 协议栈中的应用协议大多数以明文形式在网络上传输，在这些明文数据中往往包含一些敏感信息(如账号、密码等)，使用 Sniffer 可以监听到所有局域网内的数据通信，并得到这些敏感信息。

Sniffer 的隐蔽性好，它只是被动接收数据，不向外发送数据，所以在传输数据过程中，根本无法察觉。Sniffer 的局限性是只能在局域网的冲突域中进行，或者是在点到点

连接的中间节点上进行监听。

3.1.4.2 网络嗅探器

网络嗅探器在当前网络技术中使用得非常广泛。网络嗅探器既可以作为网络故障的诊断工具，也可以作为监听工具。传统的网络嗅探技术是被动地监听网络通信、用户名和口令，而新的网络嗅探技术开始主动地控制通信数据。大多数的嗅探器至少能够分析下面的协议：标准以太网、TCP/IP、IPX、DECNET 等。

根据功能不同，嗅探器可以分为通用网络嗅探器和专用嗅探器。前者支持多种协议，如 Tcpdump、Snifferit 等；后者一般是针对特定软件或提供特定功能，如专门针对 MSN 等即时通信软件的嗅探器、专门嗅探邮件密码的嗅探器等。

3.1.4.3 嗅探技术分类

根据工作环境和工作原理不同，嗅探技术又可以分为本机嗅探、广播网嗅探、交换机嗅探等类型。

1. 本机嗅探

本机嗅探是指在某台计算机内，嗅探程序通过某种方式，获取发送给其他进程的数据包的过程。例如，当邮件客户端在收发邮件时，嗅探程序可以窃听到所有的交互过程和其中传递的数据。

2. 广播网嗅探

广播网是基于集线器(Hub)的局域网络，其工作原理是基于总线方式的，所有的数据包在该网络中都会被广播发送(即发送给所有端口)。在广播网中，每一个网络数据包都被发送到所有的端口，然后由各端口所连接的网卡来判断是否需要接收，所有目的地址与网卡实际地址不符的数据包将被网卡驱动自动丢弃，这确保了广播网中每台主机只接收到以自己为目标的数据包。

广播网嗅探利用了广播网“共享”的通信方式。在广播网中所有的网卡都会收到所有的数据包，只要将本机网卡设为混杂模式，就可以使嗅探工具支持广播网或多播网的嗅探。

3. 交换机嗅探

交换机的工作原理与 Hub 不同，它不再将数据包转发给所有的端口，而是通过“分组交换”的方式进行单对单的数据传输。即交换机能记住每个端口的 MAC 地址，根据数据包的目的地址选择目的端口，只有对应该目的地址的网卡能接收到数据。

基于交换机的嗅探是指在交换环境中，通过某种方式进行的嗅探。由于交换机基于“分组交换”的工作模式，因此，简单地将网卡设为“混杂”模式并不能嗅探到网络上的数据包，必须采用其他方法来实现基于交换机的嗅探。

4. 端口镜像嗅探

端口镜像也称做巡回分析端口(roving analysis port)，它从网络交换机的一个端口转发每个进出分组的拷贝到另一个端口，分组将在此端口进行分析，端口镜像是监视网络通信量和通信内容的一种方法。网络管理员将端口镜像作为一种诊断或调试的工具，尤其是在分析网络情况的时候，它使管理员能跟踪交换机的性能并在必要时对其更改。

端口镜像是交换机为调试预留的功能。通过端口镜像,可以将交换机中任意端口的数据复制给镜像端口,本机嗅探工具就可以嗅探交换机上的任意端口了。

基于端口镜像的嗅探受限于交换机能够支持的镜像功能,能够镜像多少端口、镜像出来的协议如何都取决于交换机的型号和配置。由于进行基于端口镜像的嗅探必须拥有交换机的管理权限,因此,基于端口镜像的嗅探往往是网络管理员常用的嗅探方式。

5. 通过 MAC 泛滥进行交换机嗅探

这种方式往往被攻击者使用。网络交换机为了能够进行分组交换,必须在内部维护一个转换表,将不同的 MAC 地址转换成交换机上的物理端口。由于交换机的工作内存有限,如果用虚假的 MAC 地址对交换机进行不断攻击,直到交换机的工作内存被占满,交换机就进入了所谓的“打开失效”模式,开始了类似于集线器的工作方式,向网络上所有的机器广播数据包。在这种情况下,交换机嗅探就可以同样采用广播网嗅探的方式实现。

3.1.4.4 嗅探的安防作用

1. 网络安全审计

网络审计是指通过网络嗅探工具,将网络数据包捕获、解码并加以存储,以备后期查询或提供即时报警。通过嗅探技术,网络审计可以实现上网行为审计、网络违规数据的监控等功能。利用网络嗅探技术开发的网络行为审计类软件是运行在关键的网络节点,对网络传输的数据流进行合法性检查的工具。

2. 蠕虫病毒的控制

采用嗅探技术,对蠕虫病毒的控制可起到以下作用:

(1) 基于网络嗅探的流量检测,及时发现网络流量异常,并根据已经建成的流量异常模型,初步判断出网络蠕虫病毒爆发的前兆。

(2) 基于网络嗅探的网络协议分析,进一步确认蠕虫病毒的发作,并及时给出预警信息。

(3) 基于网络嗅探技术的蜜罐,尽早捕获蠕虫病毒的样本,并通过对其进行详细的分析,制定出有效的防御方案和清除方案。

(4) 通过基于网络嗅探技术的入侵检测,能够准确定位局域网络中的蠕虫病毒传播源,从而及时扼杀蠕虫病毒的传播行为。

3. 网络布控与追踪

针对网络犯罪,如黑客入侵、拒绝服务攻击等,通过嗅探技术进行追踪,协助执法部门定位网络犯罪分子。现代网络犯罪往往采用跳板进行,即通过一台中间主机进行网络攻击和犯罪活动,这对犯罪分子的捕获造成了很大的障碍,而嗅探技术可以有效地帮助执法人员解决这一问题。

网络追踪是针对伪造 IP 地址攻击的一种追查方法。由于网络攻击往往采用虚假的 IP 地址(特别是大规模的拒绝服务攻击),因此,从被攻击机嗅探获取的数据无法直接判断攻击源,需要采用移动的网络嗅探器,以溯源的方式从终点逐个前溯,直到发现攻击的起源点。

当发现某网络犯罪行为是通过中间跳板主机进行时,暂时不对该主机进行明显的操作,而是运行网络嗅探器对其进行 24 小时的监控,一旦犯罪分子远程登录该主机,网络嗅

探器就会记录该犯罪分子的 IP 地址，从而协助定位和追踪。目前，国内已经有多例通过网络布控和追踪的方式抓获犯罪分子的案例，其中也往往涉及嗅探技术的应用。

4. 网络取证

基于嗅探的网络取证工具可以运行在需要取证的犯罪分子所使用的计算机上（如个人计算机或公共场所的计算机），并可以将该犯罪分子的网络行为（如邮件、聊天信息、上网记录等）加以实时记录，从而协助案件的侦破和起诉证据的获取。为了确保利用嗅探工具所获得的网络证据具备不可篡改性，网络取证工具中还需要内置数字签名工具，防止操作人员人为修改或误删数字证据。

嗅探技术在黑客攻防技术及信息安全体系建设中都起到了非常重要的作用，而反嗅探技术也是确保网络私密性的关键之一。同时，嗅探技术在网络安全管理工作中也具有很大的帮助。但是，在进行嗅探技术的合法应用的同时，还需要关注嗅探技术滥用带来的泄密和破坏个人隐私问题。在未来，随着网络技术的发展，嗅探技术和反嗅探技术还将不断进步，目前在高速化、可视化、针对加密的嗅探和无线切入技术四个方向上都可以见到新技术的出现。

3.2 Sniffer 网络分析实例

3.2.1 Sniffer Pro 简介

Sniffer Pro 软件是 NAI 公司推出的功能强大的协议分析软件。利用 Sniffer Pro 网络分析器的强大功能和特征，解决网络问题。本教材使用的软件版本为 SnifferPro_4_70_530。

Sniffer Pro 软件的主要作用可以体现在以下方面：

（1）Sniffer 可以评估业务运行状态，如各种应用的响应时间，一个操作需要的时间，应用带宽的消耗，应用的行为特征，应用性能的瓶颈等。

（2）Sniffer 能够评估网络的性能，如各链路的使用率，网络性能趋势，消耗最多带宽的具体应用，消耗最多带宽的网络用户，各分支机构流量状况，影响网络性能的主要因素。

（3）Sniffer 可以快速定位故障，monitor、expert、decode 等功能都可以快速定位故障。

（4）Sniffer 可以排除潜在的威胁，如病毒、木马、扫描等，并且发现攻击的来源，为控制提供根据，对蠕虫类型等对网络影响大的病毒有效。作为即时监控工具，Sniffer 通过发现网络中的行为特征来判断网络是否有异常流量，所以 Sniffer 可能比防病毒软件更快发现病毒。

（5）Sniffer 可以做流量的趋势分析，通过长期监控，可以发现网络流量的发展趋势，为将来网络改造提供建议和依据。

（6）应用性能预测。Sniffer 能够根据捕获的流量分析一个应用的行为特征，可以提供量化的预测，准确率较高，误差不超过 10％。

Sniffer 包括四大功能：监控（monitor）、显示（display）、数据包捕捉（capture）和专家分析系统（expert）。

3.2.2　程序安装实验

实验器材

- Sniffer Pro 软件系统 1 套。
- PC(Windows XP/Windows 7)1 台。

预习要求

- 做好实验预习,复习网络协议有关内容。
- 熟悉实验过程和基本操作流程。
- 做好预习报告。

实验任务

通过本实验,学会在 Windows 环境下安装 Sniffer;能够运用 Sniffer 捕获报文。

实验环境

本实验采用一个已经连接并配置好的局域网环境。PC 上安装 Windows 操作系统。

预备知识

- TCP/IP 原理及基本协议。
- 数据交换技术概念及原理。
- 路由技术及实现方式。

实验步骤

按照常规安装方法双击 Sniffer 软件的安装图标,按顺序进行(如图 3.3 所示),本教材选用的软件版本为 Sniffer Portable 4.7.5。



图 33　软件安装界面

如图 3.4 所示,在选择 Sniffer Pro 的安装目录时,默认安装在 C:\Program Files\NAI\SnifferNT 目录中,为了更好地使用,建议用默认路径进行安装。



图 34　安装目录选择界面

在注册用户时，需要填写必要的注册信息。在出现的 Sniffer Pro User Registration 的三个对话框中，依次填写个人信息。如图 3.5 所示，注意最后一行的 Sniffer Serial Number 需要填入软件购买时提供的注册码。



图 35　用户注册界面

如图 3.6 所示，完成注册操作后，需要设置网络连接状况。从上至下，依次有三个选项：Direct Connection to the Internet（直接连接）、Connection to the Internet through a Proxg（通过代理服务器连接）、Not connected to network or dial-up. Print & fax option（拨号、传真或无连接）。一般情况下，用户直接选择第一项。

如图 3.7 所示，若通过代理服务器连接，则需要输入代理服务器地址、用户名和账号等信息。

接下来，系统会自动定位并连接到最近的网络服务器 Mercury. nai. com，完成必要的注册信息提交和注册码认证工作。当用户的注册信息验证通过后，系统会转入如图 3.8 所示的界面，用户被告知系统分配的身份识别码，以便用户进行后续的服务和咨询。

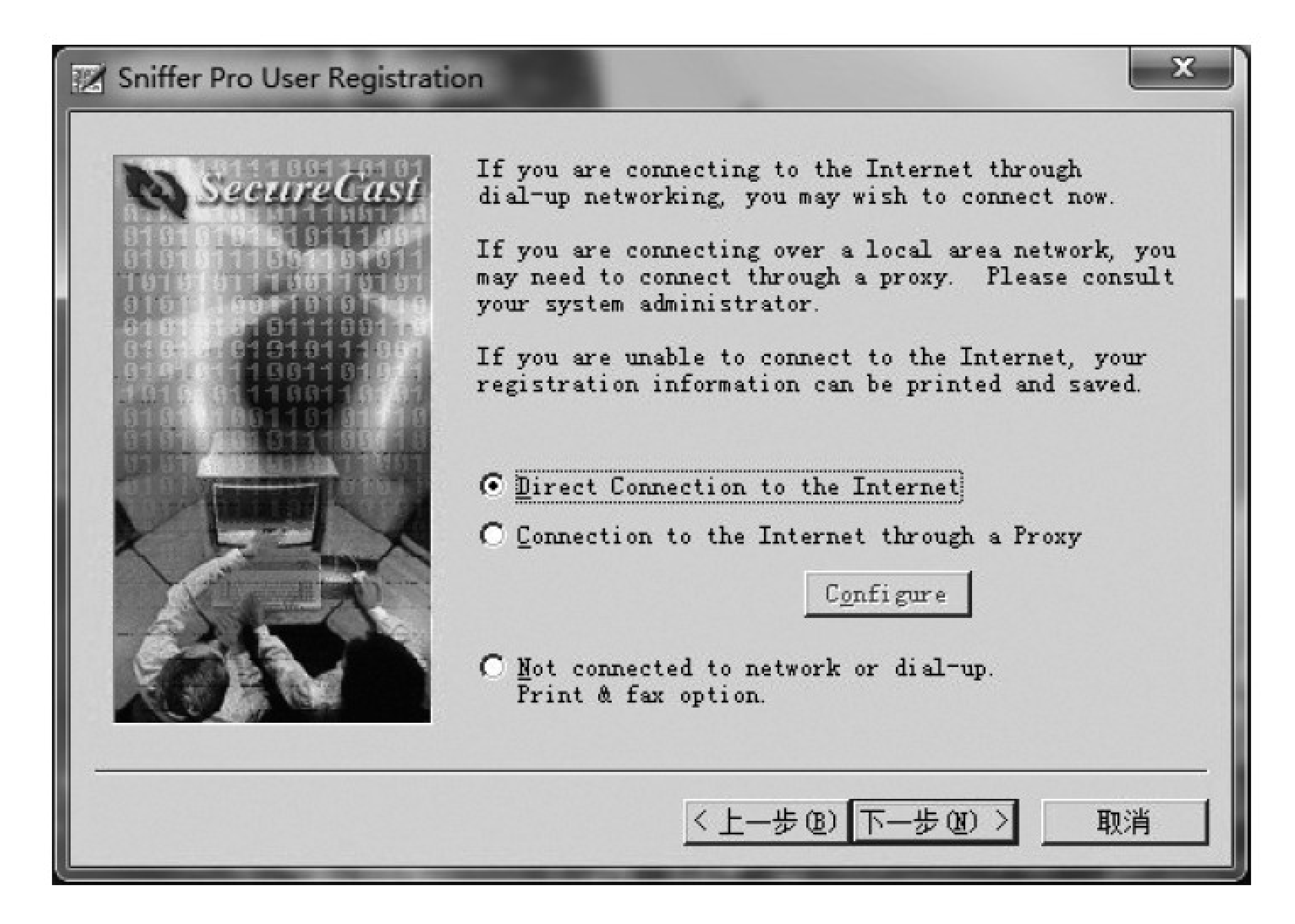


图 36　网络连接状况设置界面

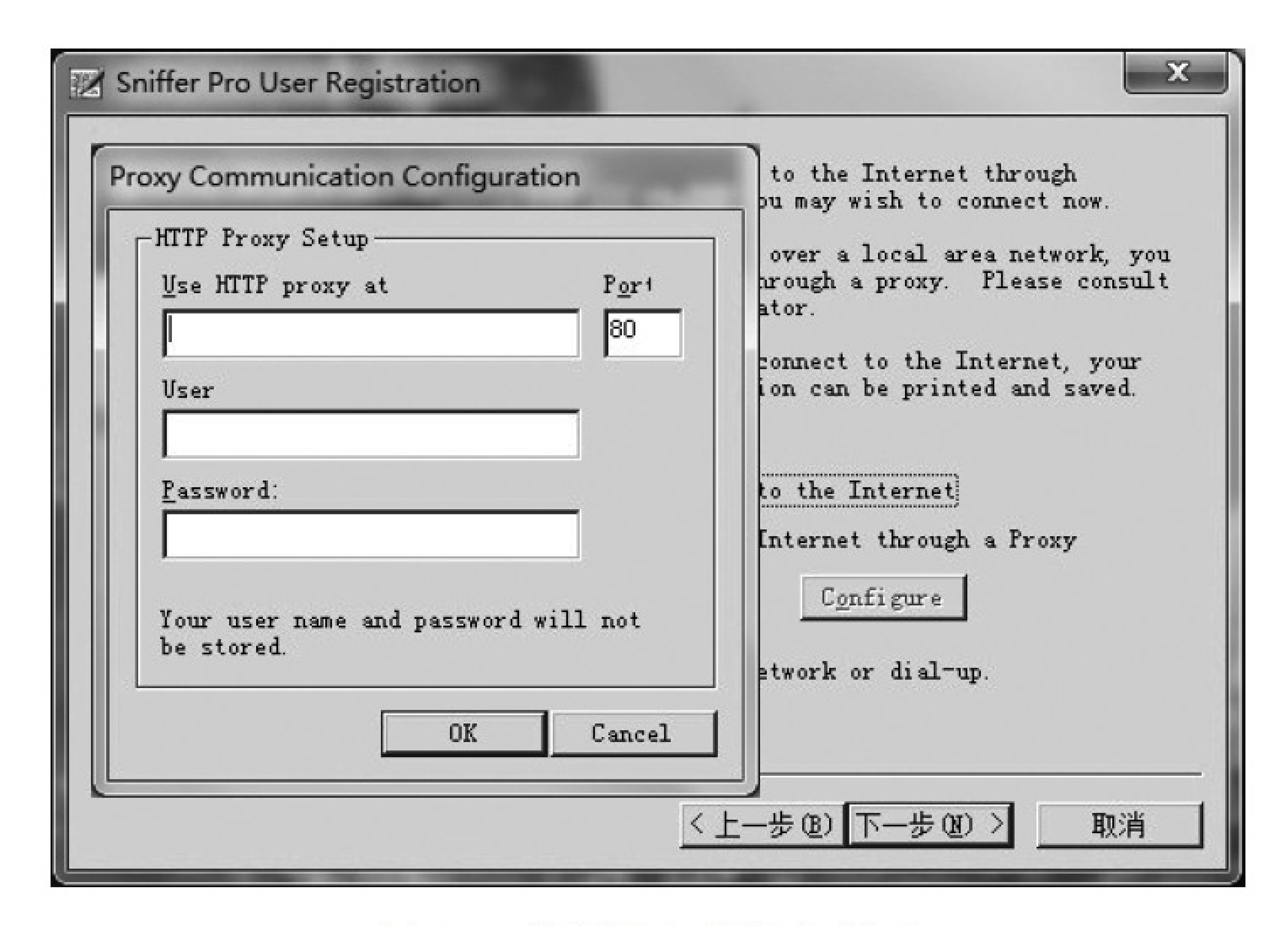


图 37　代理服务器设定界面

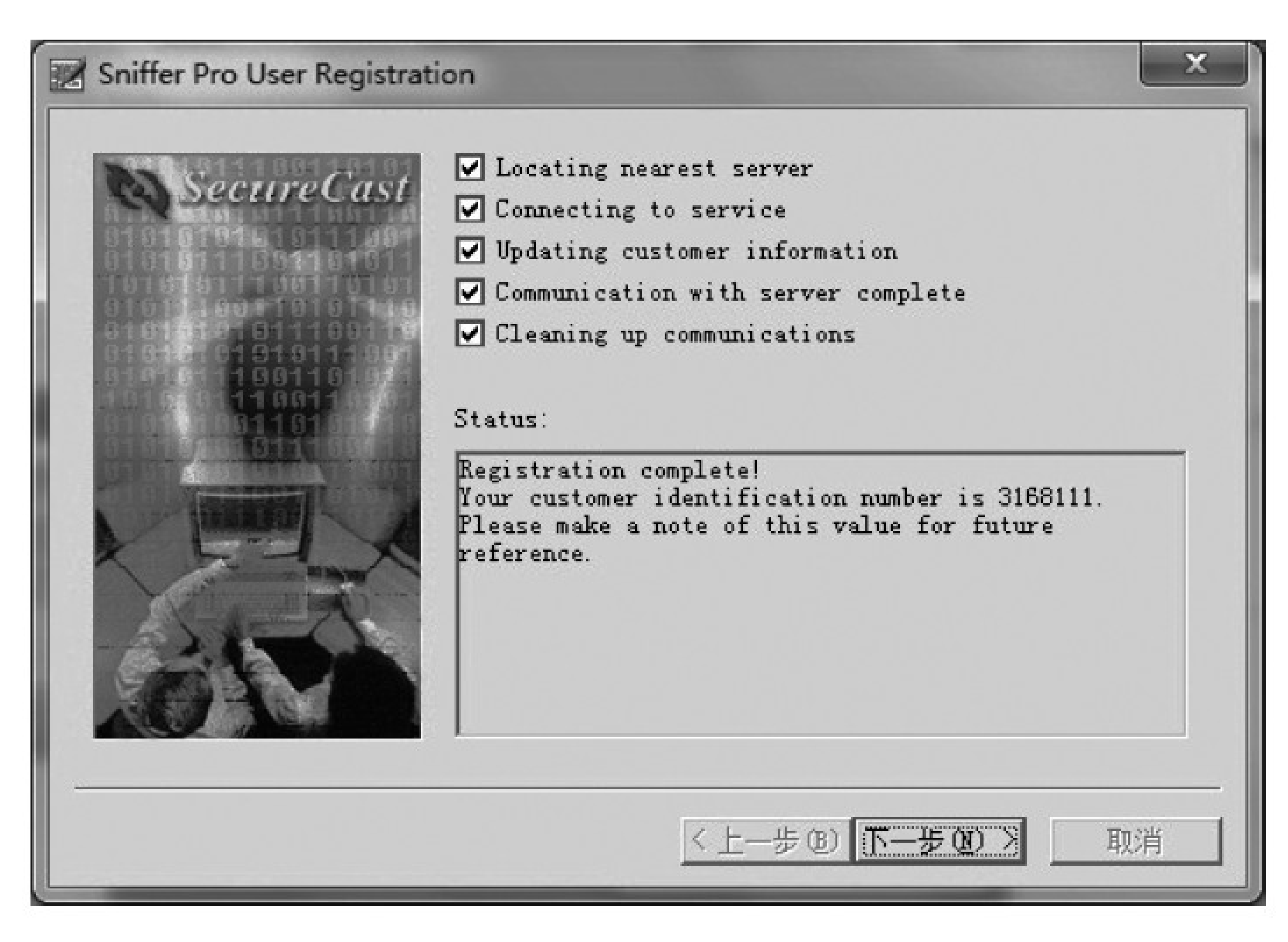


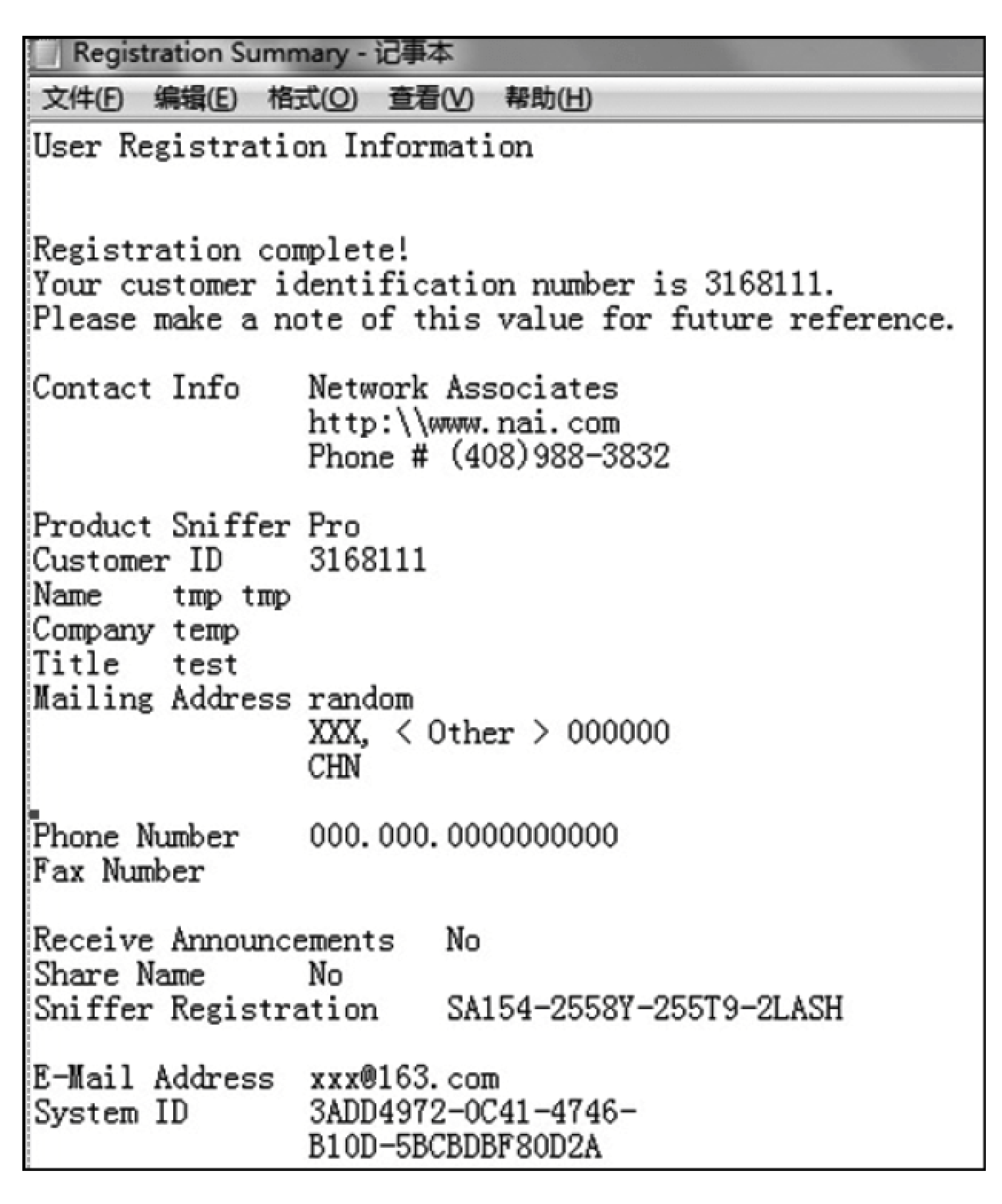
图 38　注册信息验证界面

此时，用户单击“下一步”按钮时，系统会提示用户保存关键性的注册信息，并生成一个文本格式的文件 Registration Summary. txt，如图 3. 9 所示。该文件主要包括了以下几个重要部分，详细内容可参照图 3. 10。

- customer identification number(用户身份识别码)。
- Contact Info(服务器连接信息)。
- Product Sniffer Pro(用户填写的身份注册信息)。



图 3.9　注册信息保存提示



```
Registration Summary - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
User Registration Information


Registration complete!
Your customer identification number is 3168111.
Please make a note of this value for future reference.

Contact Info        Network Associates
                    http:\\www.nai.com
                    Phone # (408)988-3832

Product Sniffer Pro
Customer ID         3168111
Name        tmp tmp
Company temp
Title       test
Mailing Address random
                    XXX, < Other > 000000
                    CHN

Phone Number        000.000.0000000000
Fax Number

Receive Announcements       No
Share Name          No
Sniffer Registration        SA154-2558Y-255T9-2LASH

E-Mail Address      xxx@163.com
System ID           3ADD4972-0C41-4746-
                    B10D-5BCBDBF80D2A
```

图 3.10　注册文件内容

由于 Sniffer Pro 软件的运行环境需要 Java 环境支持,因此,在软件使用前安装程序会提示用户安装并设置 Java 环境(如图 3.11 所示)。

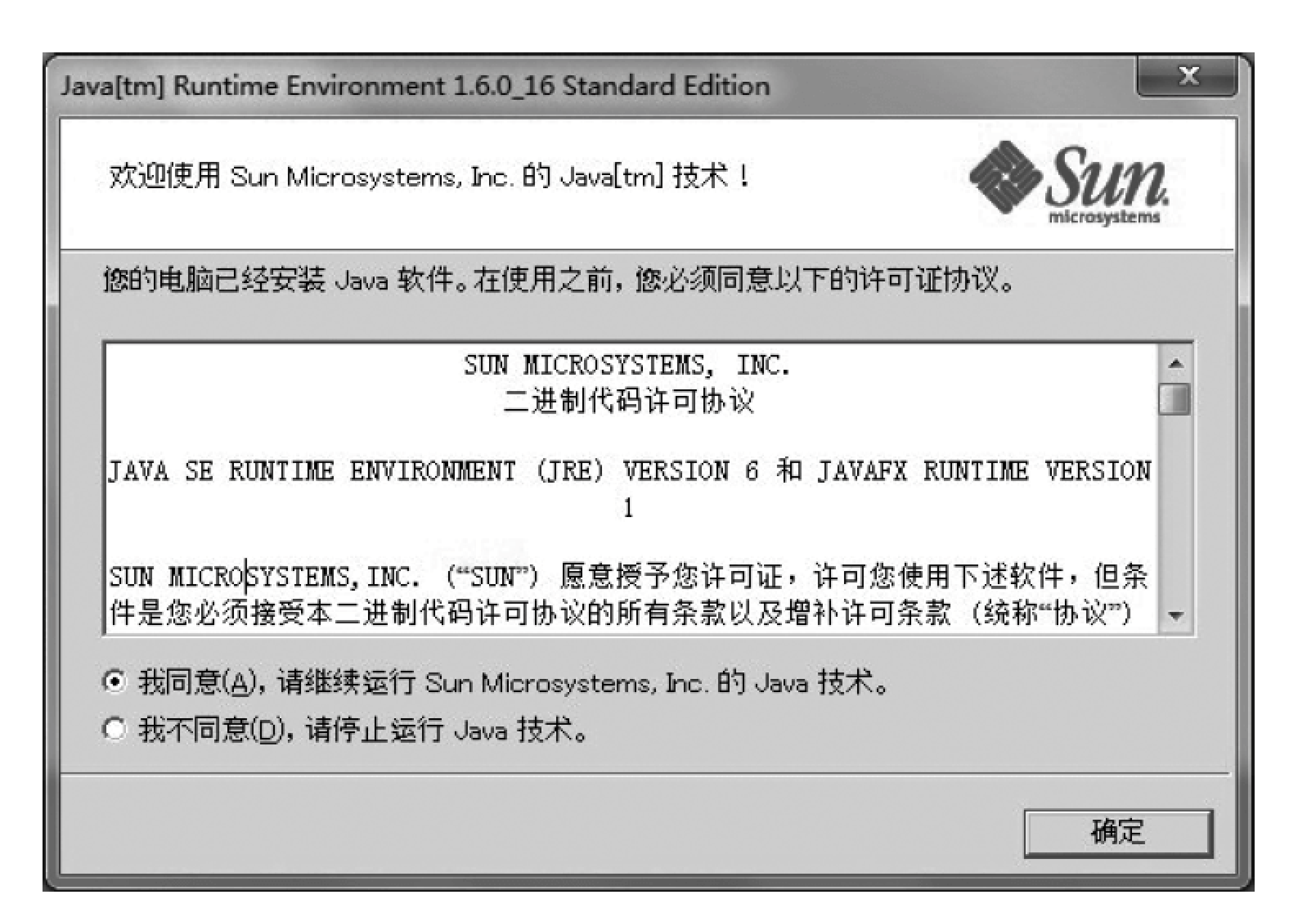


图 3.11 设置 Java 环境

接下来,系统在完成关键文件复制和安装的工作后,会出现 Setup Complete 提示,由于 Sniffer Pro 需要将网卡的监听模式切换为混杂,所以需要重新启动计算机来完成网卡的工作模式切换,当软件提示重新启动计算机时,按照提示操作即可。

重新启动计算机后,可以通过运行 Sniffer Pro 来监测网络中的数据包。通过选择"开始"|"程序"|Sniffer Pro-Sniffer 来启动程序。在进入主界面后,首先要配置监听网卡。一般情况下,Sniffer Pro 初次运行时会自动选择机器网卡进行监听。如果本地计算机有多个网卡时,则需要手工指定。具体方法如下:

(1) 选择 File 下的 Settings Select 选项。

(2) 在 Select Settings 窗口中选择监听的网卡,同时选择 Log Off 复选框,单击"确定"按钮,如图 3.12 所示。

(3) 如果存在多个网卡,则需要确定最终的监听网卡,如图 3.13 所示。



图 3.12 设置提示

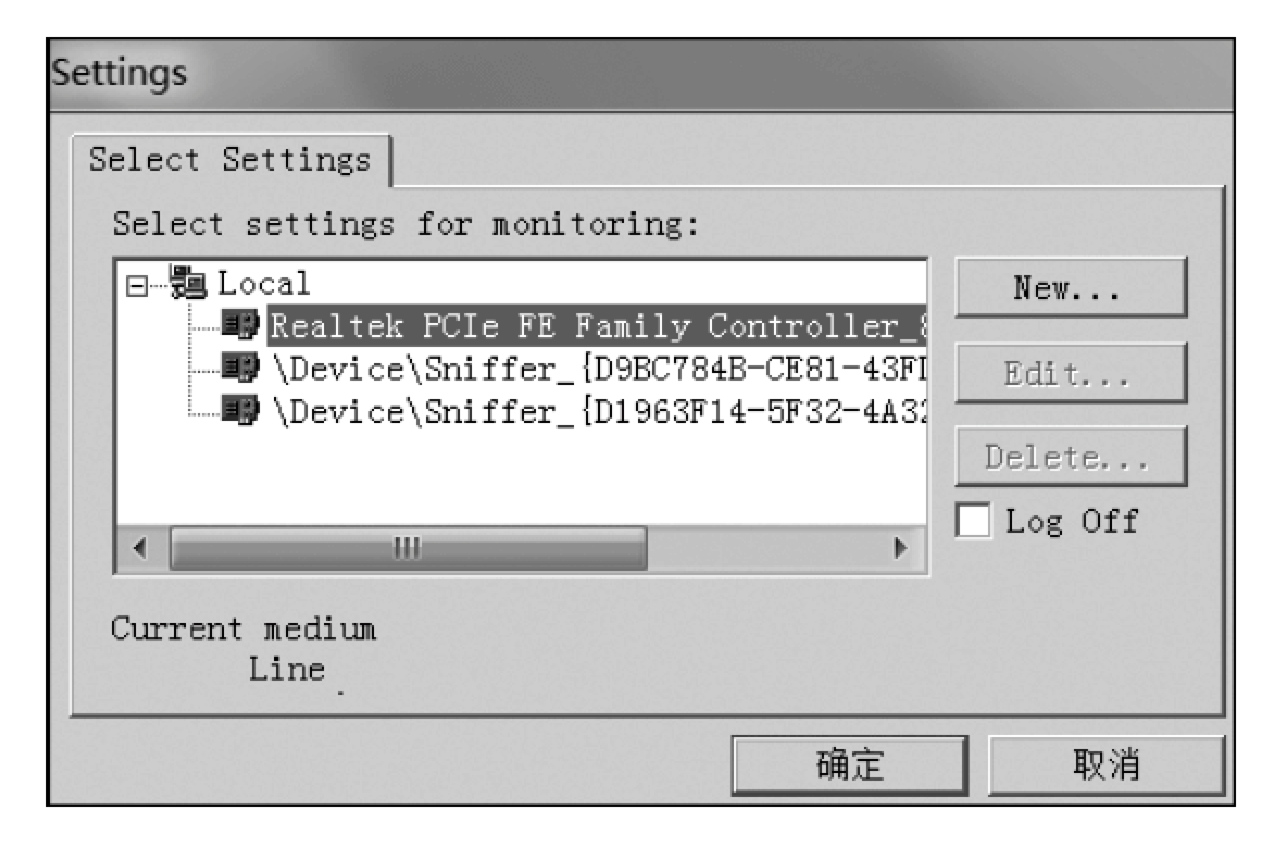


图 3.13 多网卡设置提示

完成上述操作后,就可以使用 Sniffer Pro 对目标机器进行网络监听,如图 3.14 所示,快捷操作功能主要包括报文捕获及网络性能监视,主要监控目标机器的网络流量和错误数据包情况。网络监听的主要参考指标包括网络使用率(Utilization)、数据包传输率(Packets/s)、错误数据情况(Error/s)。



图 3.14　快捷操作菜单

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

思考题

(1) 网卡的工作模式有几种?

(2) 阐述监听模式的具体工作情况。

3.2.3　数据包捕获实验

实验器材

- Sniffer Pro 软件系统 1 套。
- PC(Windows XP/Windows 7)1 台。

预习要求

- 做好实验预习,复习网络协议有关内容。
- 熟悉实验过程和基本操作流程。
- 做好预习报告。

实验任务

通过本实验,熟练掌握 Sniffer 数据包捕获功能的使用方法。

实验环境

本实验采用一个已经连接并配置好的局域网环境。PC 上安装 Windows 操作系统。

预备知识

- 数据交换技术的概念及原理。
- 路由技术及实现方式。

实验步骤

1. 报文捕获

数据包捕捉(capture)是将所有的数据包截取并放在磁盘缓冲区中,便于分析。基本

原理就是通过软件手段设置网络适配器(NIC)的工作模式,在这种模式下网卡接收所有的数据,达到网络监控和网络管理的功能。

如图 3.15 所示,报文捕获快捷操作的功能依次为开始、暂停、停止、停止显示、显示、定义过滤器以及选择过滤器,一般情况下,选择默认的捕获条件。

Sniffer 在启动后,一般处于脱机模式。在捕获报文之前,需要进入记录模式,通过选择“文件”菜单下的“记录于”来启动网卡的监听模式。也可以通过“选定设置”选择 LOG On/Off 来完成上述操作。此时,可根据需要进行局域网的回环测试。选择“捕获”菜单下的“开始”或直接单击捕获快捷菜单的“开始”按钮,系统会开始进行网络报文的捕获。

在捕获过程中,单击快捷菜单中的“捕获面板”或选择“捕获”菜单下的“捕获面板”选项,可以随时查看捕获报文的数量以及数据缓冲区的利用率,如图 3.16 所示。

图 3.15 捕获报文快捷操作菜单

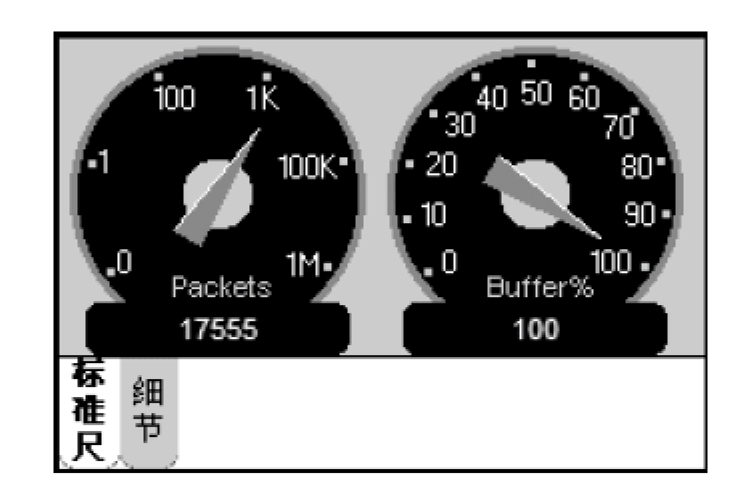


图 3.16 报文捕获面板

左侧仪表显示了系统当前捕获到的报文数量,右侧仪表显示了捕获报文的数据缓冲大小。此外,还可以选择“细节”功能,查看详细的统计信息,如图 3.17 所示。

Status			
# 看见	60030	# 已接受的	22003
# Drops	0	# 拒绝	0
缓冲器大小	8 MB	碎片大小	全部
缓冲器动作	覆盖	逝去时间	0:14:31
保存文件#	N/	文件覆盖	N/

标准尺 细节

图 3.17 报文捕获统计信息

捕获到的报文存储在缓冲区内。使用者可以显示和分析缓冲区内的当前报文,也可以将报文保存到磁盘,加载和显示之前保存的报文信息,进行离线分析和显示。

整个捕获过程受“定义过滤器”的约束,选择“捕获”菜单下的“定义过滤器”,单击“缓冲”选项卡,对捕获缓冲区进行设置。

首先,缓冲区的大小由用户自定义,根据实际主机的内存容量进行调整。缓冲区设置过大容易造成软件运行延迟。

其次,数据包大小应选择适度,截取部分数据包能够节省磁盘空间,保证网络通信流畅,避免丢失帧。

值得一提的是,当禁止“保存到文件”选项时,可以选择停止捕获条件,即缓冲区已满或覆盖原有数据。

此外,也可以通过指定文件名前缀和脱机文件数对捕获信息进行存储,如图 3.18 所示。



图 3.18　捕获缓冲区设置

以上介绍的是基本捕获方式,若需要捕获特定主机或工作站的数据包,可以通过选择“监视器”菜单的“主机列表”选项查看工作站信息,并单击单个主机进行数据包捕获。

2. 报文分析

为了有效进行网络分析,需要借助于专家分析系统。首先,应根据网络协议环境,对专家系统进行配置。选择“工具”菜单中的“专家选项”,如图 3.19 所示。

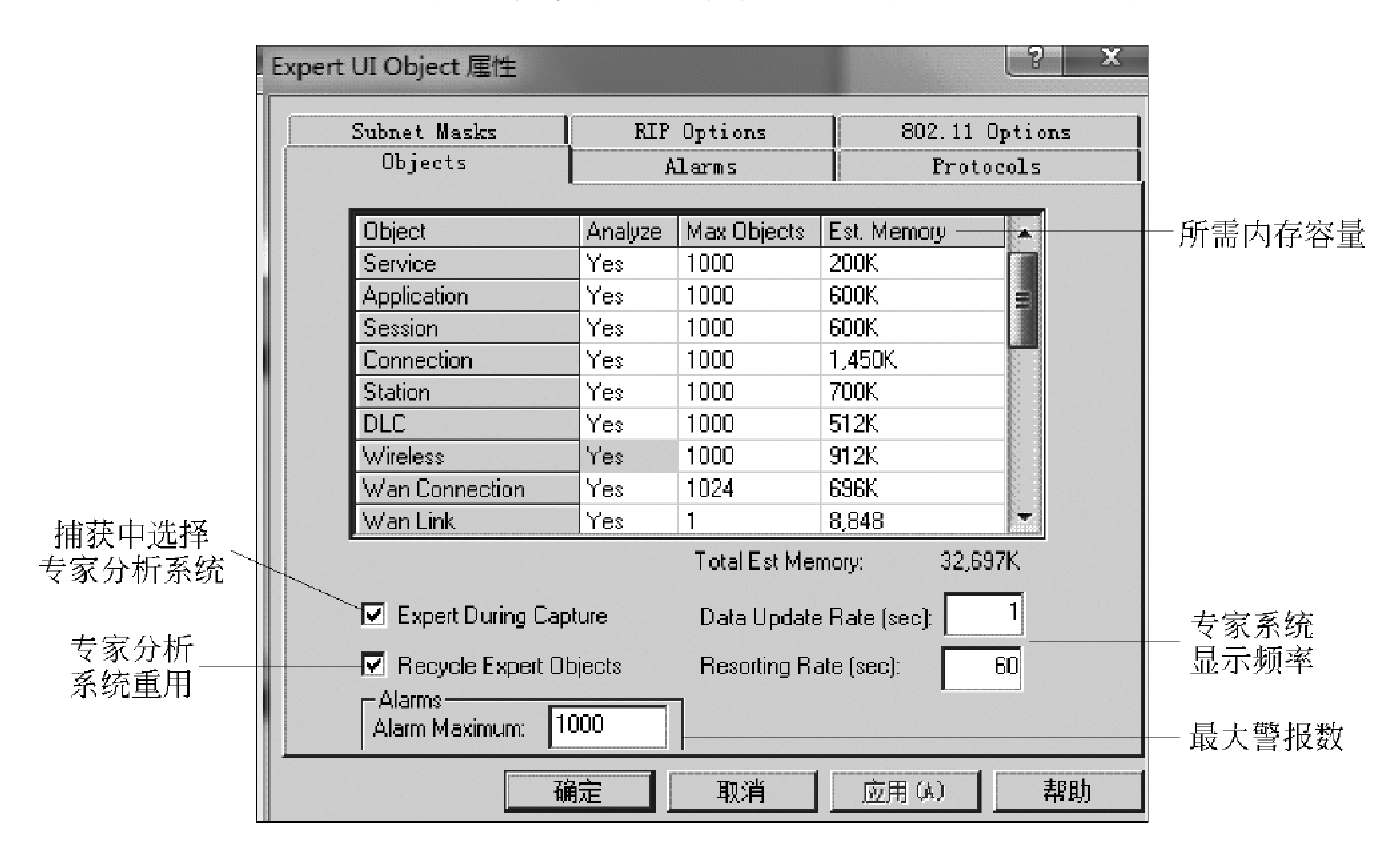


图 3.19　专家选项设置

专家系统的配置能够帮助分析人员专注于特定问题,通过排除某些系统层数据,捕获到网络分析所需的特定通信量。同时,根据每层对象所需的内存容量,来创建每个系统层的最大对象数。

专家系统提供了多种功能和配置选项,具体如下。

- 在专家系统的设置操作中,“专家系统重用”选项定义了当内存不足时专家系统需要进行的操作,即覆盖原有数据来创建新对象(选中)或停止创建对象,对已有数据进行分析(未选中)。

- 默认情况下，当数据包捕获开始时，专家系统就开始分析进入缓冲区的数据包，并在窗口中实时显示，用户可以在捕获的同时分析网络对象、症状，并作出诊断。用户也可以选择禁用实时分析功能（未选中）。
- 指定可创建的最大警报数。当达到最大警报数时，专家系统会覆盖最早最低级别的警报（选中）或者停止创建警报。
- 专家系统显示的刷新频率，以及专家系统由数据分析操作到数据显示操作之间的延迟。
- 对于专家系统的警报阈值配置，可以选择“工具”菜单下的“专家选项”中的“警报/Alarms”进行具体设置。

值得注意的是，系统默认的阈值都是经过精确计算的，可保证系统进行诊断和问题检测需求，对于阈值的修改，可能会导致系统判断失误或运行错误。如图 3.20 所示，对于每一个系统层存在多个症状诊断的警报阈值信息。

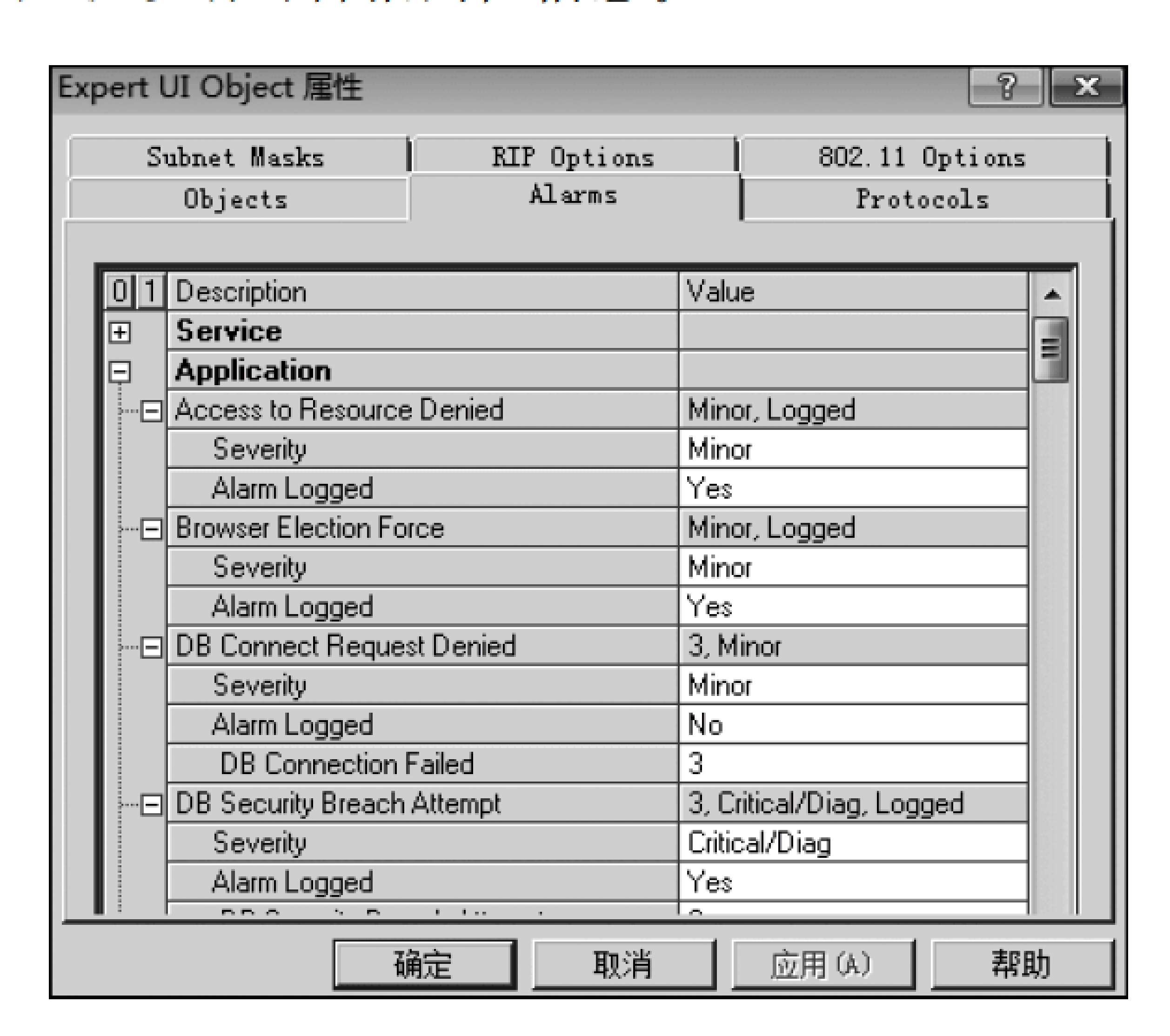


图 3.20　专家系统阈值设置

对于各类网络协议，用户可以进行选择性的监听和分析，单击“警报/Alarms”右侧的“协议/Protocols”设置项，如图 3.21 所示，可按照系统分析层进行协议选择。

此外，当网络使用了不规范的子网掩码时，可以通过选择“子网掩码/Subnet Masks”设置项进行更改。

在专家系统中，还为用户提供了用于检测路由故障的路由信息协议分析（RIP），通过分析所捕获报文的路由选择协议来构建路由表并显示。专家系统通常会发现网络上的默认路由器，同时构建一条通向网关的默认静态路由。如果选择使用 RIP 分析方式，则需要将“对象”设置项中的连接层和应用层定义为“分析”，如图 3.22 所示。

在专家系统属性设置中，还特别设定了用于无线网络分析的选项。在启用欺诈 AP 查找的选项后，专家系统就会对访问主机的 MAC 地址和选项中已存地址进行比较，一旦出现异常就会生成警报。

通过“显示”菜单下的“显示设置”选项，可以自定义要显示的分析内容。如图 3.23 所示，主要包括如下方面。

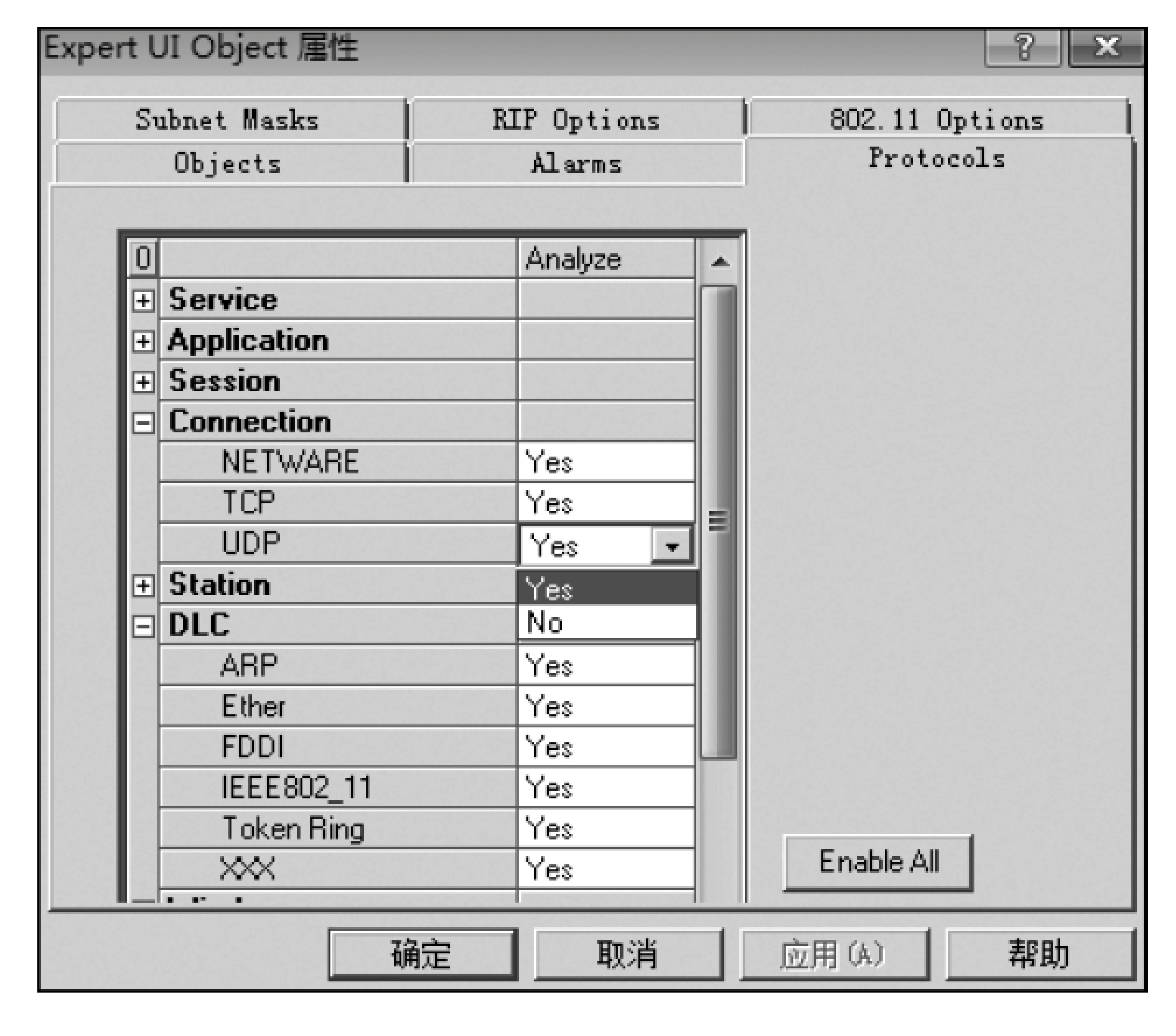


图 3.21　指定分析协议设置

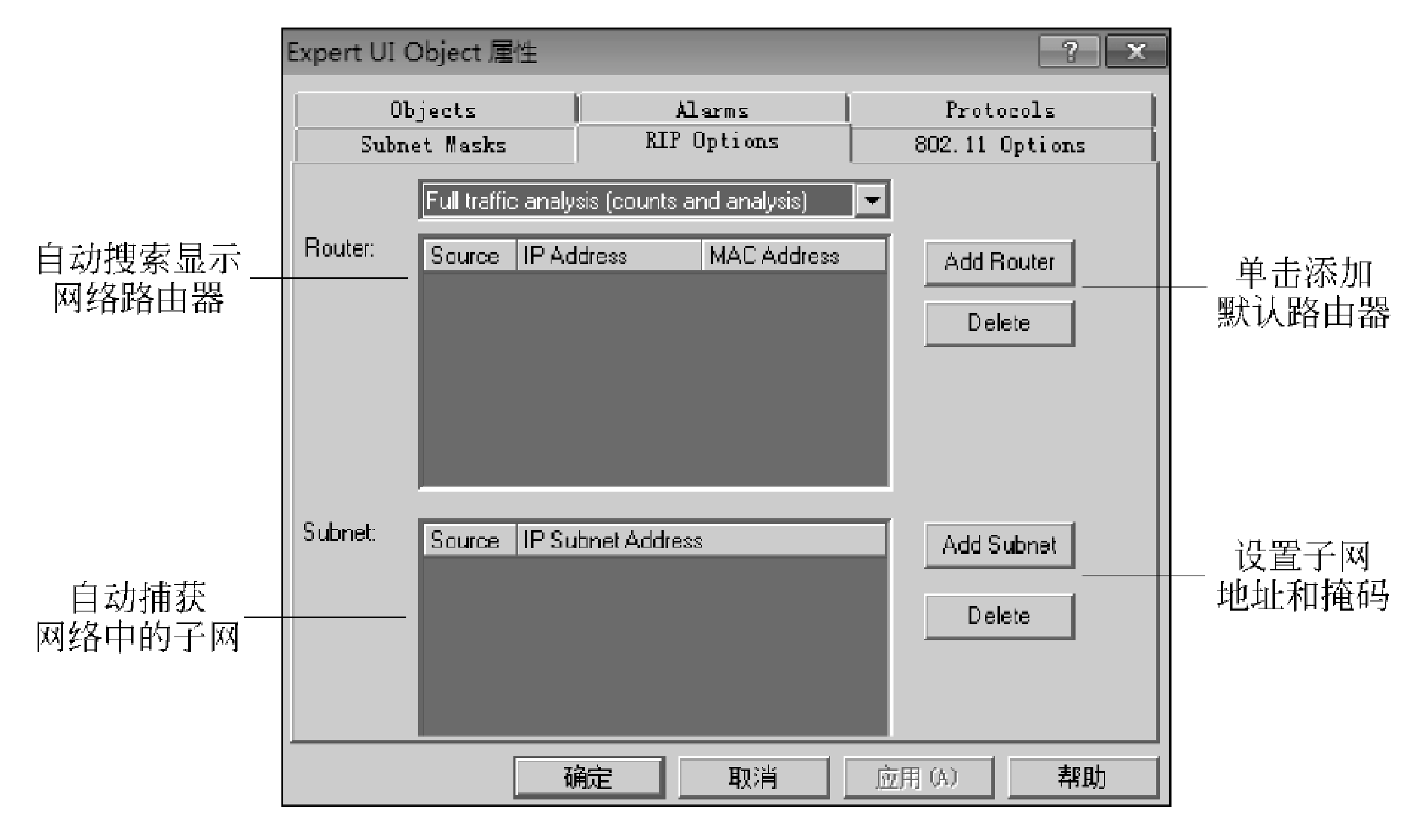


图 3.22　指定分析协议设置



图 3.23　摘要显示设置

• 普通：可以显示或隐藏“主机列表”、“矩阵”、“协议分布”、“统计数据”等。
• 摘要显示：可以定义具体显示的专家症状、系统层等内容。
• 协议颜色：可以改变显示协议所使用的字体颜色。
• 协议使详诉：可以设置每个协议的详细显示设置。
• 解码字体：可以更改“解码”显示中文本字体类型、颜色和大小。

具体摘要显示选项如表 3.1 和表 3.2 所示。

表 3.1 摘要显示选项说明

显 示 选 项		启用功能描述
关键区域信息	专家系统症状	为每个帧显示所发现的上一个症状
	全部层	显示帧中所包含的协议层，每个协议层一行
	网络地址	显示为网络地址，否则为硬件地址
	MAC 地址中的厂商 ID	在 MAC 地址的开头部分显示供应商名称
	网络地址的名称解析	显示网络地址的名称，而不是数字地址
	地址簿解析名称	如果工作站在地址簿中已命名，则显示其名称，而不是地址
	二进制格式	显示将表示为两个窗口，以显示工作站之间的通信情况
可选择区域	状态	当数据包出现异常时，显示异常状态表示，如表 3.2 所示
	绝对时间	显示收到帧的时间
	Delta 时间	显示当前帧和上一帧之间的时间间隔
	相对时间	显示当前帧和标记帧之间的时间间隔
	Len(字节)	显示帧的长度
	累计的字节	显示从标记帧开始，到当前帧的所有帧的长度

表 3.2 状态标志说明

状态标志	状 态 描 述	状态标志	状 态 描 述
M	数据包已标记	帧不全	数据包小于 64 字节，无 CRC 错误
A	数据包是端口 A 捕获到的	分段	数据包小于 64 字节，有 CRC 错误
B	数据包是端口 B 捕获到的	超大	数据包大于 1518 字节，无 CRC 错误
#	数据包存在症状，或具体诊断内容	冲突	数据包由于冲突而损坏
触发器	数据包是一个数据触发器	对齐	数据包长度不是 8 的整数倍
CRC	具有 CRC 错误、大小正常的数据包	地址重复	在环中有地址冲突
超长	具有 CRC 错误、大小超长的数据包	帧复制	目的主机未收到数据包

在专家系统的解码显示窗口中，可以通过“显示”菜单下的“查找帧”来获得特定帧信息，“查找帧”包含四个选项。

• 文本：即搜索包含特定文本字符信息的帧。

• 数据：即搜索包含特定数据模式的帧。
• 状态：允许搜索具有特定状态标志的帧。
• 专家系统：允许搜索与特定专家系统症状或诊断关联的帧。

专家分析系统(expert)能够对缓冲区内的数据包进行综合分析，将捕获内容按照服务、应用、连接、工作站、路由、子网等类别进行分类统计，并对存在安全隐患和问题的服务或连接进行分析，给出确切的结论。对于问题内容，将注明其所属层次(layer)、诊断方式(diagnose)、基本征兆(symptom)和目标(object)。

专家分析平台可以对网络流量进行实时分析，并提供客观翔实的诊断结果，主要包括专家分析系统、解码系统、矩阵、主机列表、协议列表以及统计分析系统，只要单击“停止并显示”就可以查看具体的网络分析数据，如图 3.24 所示。

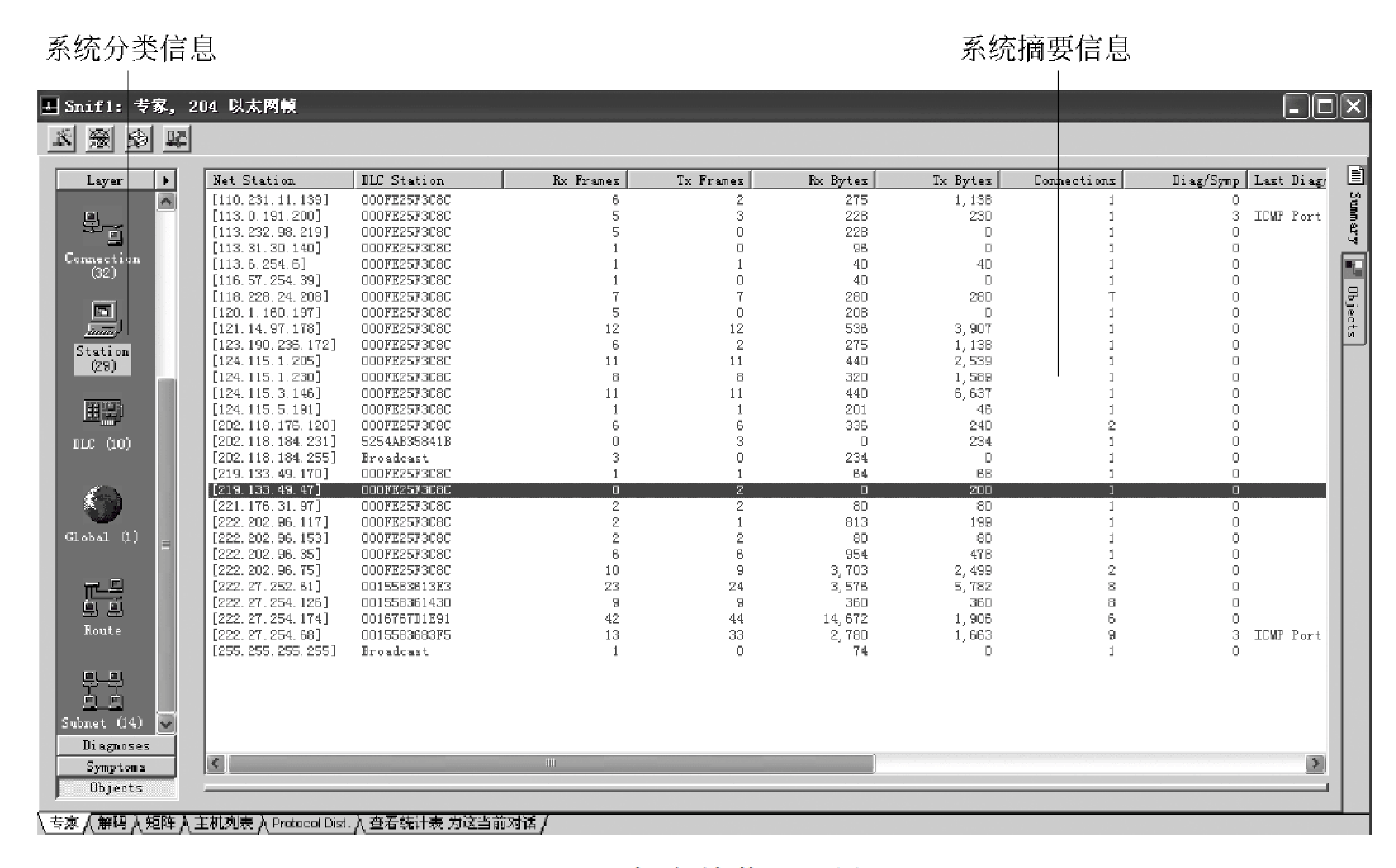


图 3.24　报文捕获显示界面

通过专家分析平台，可以捕获在网络会话过程中存在的各类潜在问题。这些问题被定义为症状或诊断。

• 症状：网络会话情况超过专家设定阈值，表示网络存在潜在问题。
• 诊断：多个一起分析的症状、复发率较高的特定症状，对于诊断必须立即检查。
• 专家系统分类信息：显示网络各个分析层，其层次性与 ISO 层相类似。
• 专家系统摘要信息：根据摘要显示设定的各层显示数据。

对于某项统计分析可以通过双击方式来查看对应记录的详细统计信息，如图 3.25 所示。对于每一项记录都可以通过查看帮助的方式来了解产生的原因。

3. 解码分析

单击专家系统下方的“解码”按钮，就可以对具体的记录进行解码分析，如图 3.26 所示。页面自上而下由三部分组成：捕获的报文、解码后的内容、解码后的二进制编码信息。



图 3.25 报文详细信息

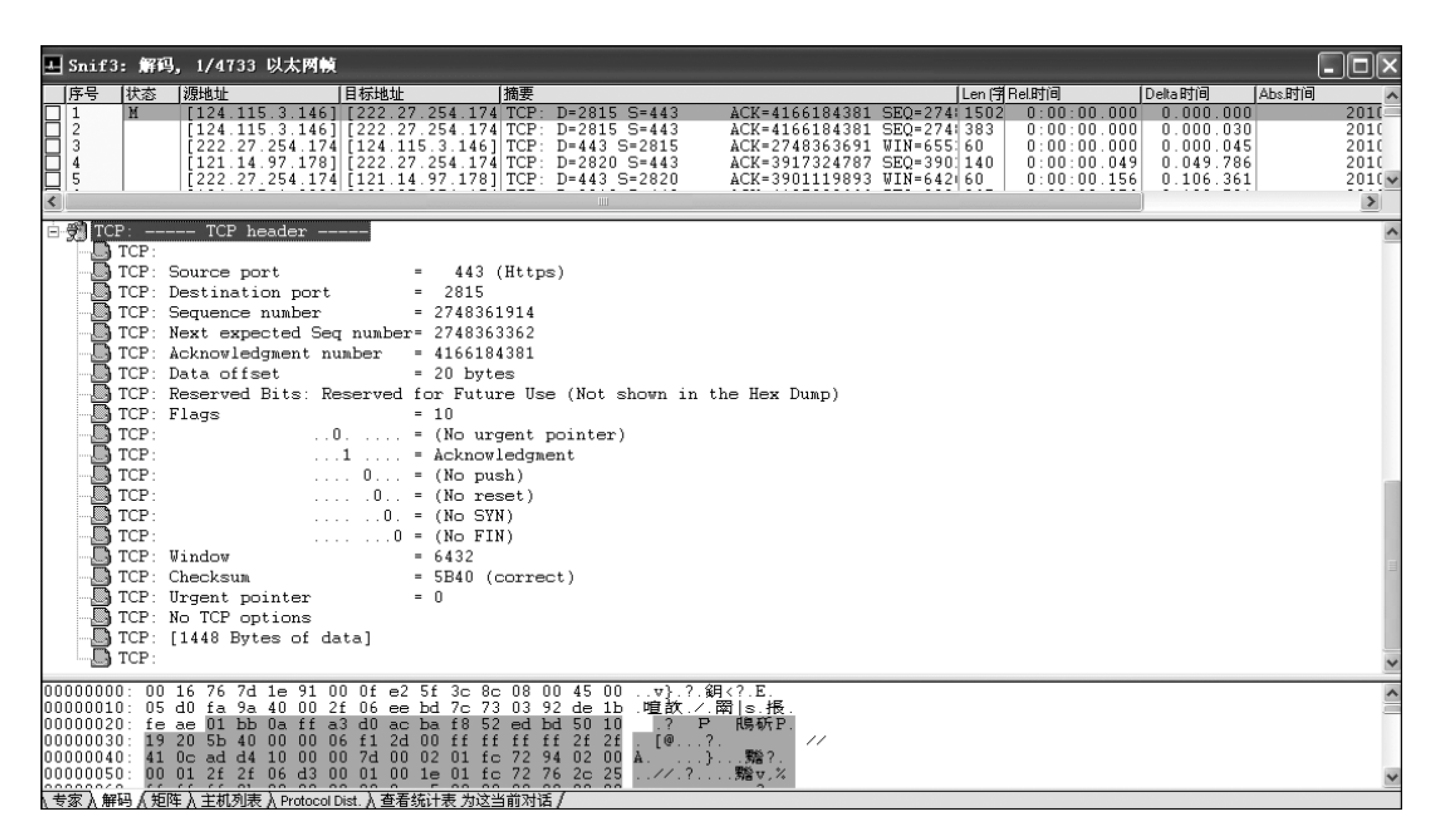


图 3.26 报文解码

对于解码分析人员来说，只有充分掌握各类网络协议，才能看懂解析出来的报文。利用软件解码分析来解决问题的关键是要对各种层次的协议有充分的了解。

4. 统计分析

对于各种报文信息，专家系统提供了矩阵(matrix)分析(如图 3.27 所示)、主机列表(host table)分析(如图 3.28 所示)、协议统计(protocol dist)分析(如图 3.29 所示)以及会话统计(statistics)分析(如图 3.30 所示)等多种统计分析功能，可以按照 MAC 地址、IP 地址、协议类型等内容进行多种组合分析。

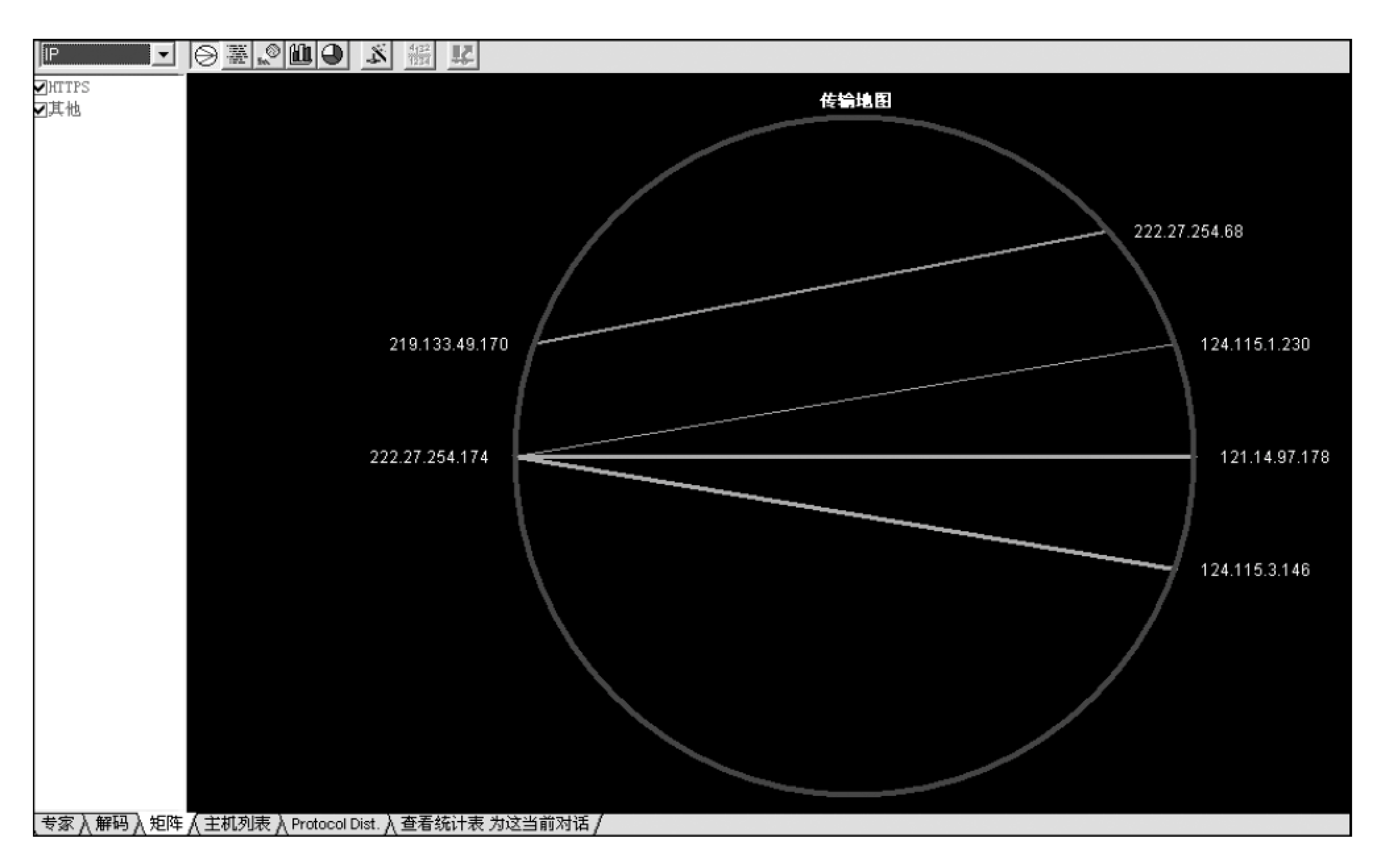


图 3.27　矩阵分析

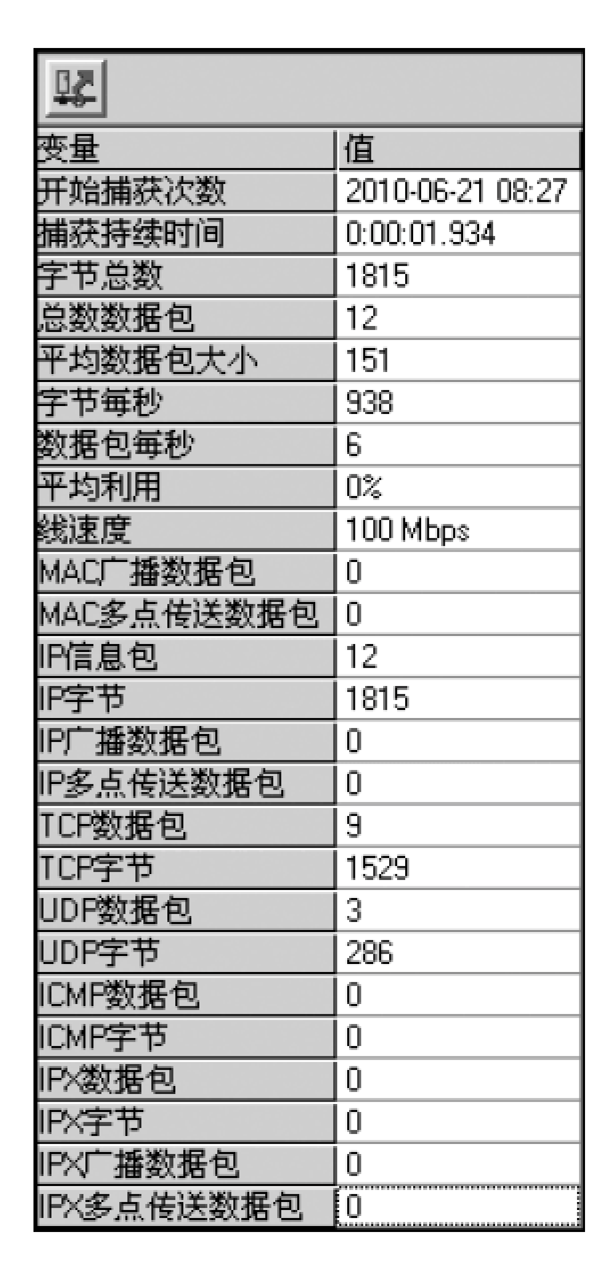
		入埠数据包	入埠字节	出埠数据包	出埠字节	数据包总数	字节总数
IP	[illegible]	4	1209	5	320	9	1529
	000FE25F3C8C	6	402	6	1413	12	1815
	本地	2	204	1	82	3	286

图 3.28　主机列表分析



协议	数据包	字节
HTTPS	9	1529
其他	3	286

图 3.29　协议统计分析



变量	值
开始捕获次数	2010-06-21 08:27
捕获持续时间	0:00:01.934
字节总数	1815
总数数据包	12
平均数据包大小	151
字节每秒	938
数据包每秒	6
平均利用	0%
线速度	100 Mbps
MAC广播数据包	0
MAC多点传送数据包	0
IP信息包	12
IP字节	1815
IP广播数据包	0
IP多点传送数据包	0
TCP数据包	9
TCP字节	1529
UDP数据包	3
UDP字节	286
ICMP数据包	0
ICMP字节	0
IPX数据包	0
IPX字节	0
IPX广播数据包	0
IPX多点传送数据包	0

图 3.30　会话统计分析

5. 捕获条件设置

在 Sniffer 环境下，可以通过“定义”的方式来对捕获条件进行设置，获得用户需要的报文协议信息。基本的捕获条件有两种。

(1) 链路层捕获：按照源 MAC 地址和目的 MAC 地址设定捕获条件，输入方式为十六进制 MAC 地址，如 000D98ABCDFE。

(2) IP 层捕获：按照源 IP 地址和目的 IP 地址设定捕获条件。输入方式为 IP 地址，如 192.168.1.157。特别注意的是，如果选择 IP 层捕获方式，则 ARP 等类型的报文信息

将被过滤掉。

用户可以通过单击快捷面板上的按钮，或选择“捕获”菜单下的“定义过滤器”来设定捕获条件，如图 3.31 所示。



图 3.31　过滤器操作界面

过滤器主要包括摘要、地址、数据模式、高级、缓冲五个操作界面。

- 摘要操作界面显示了当前缓冲器的设定情况。
- 地址操作界面用来进行缓冲器捕获条件的设定，如图 3.32 所示。

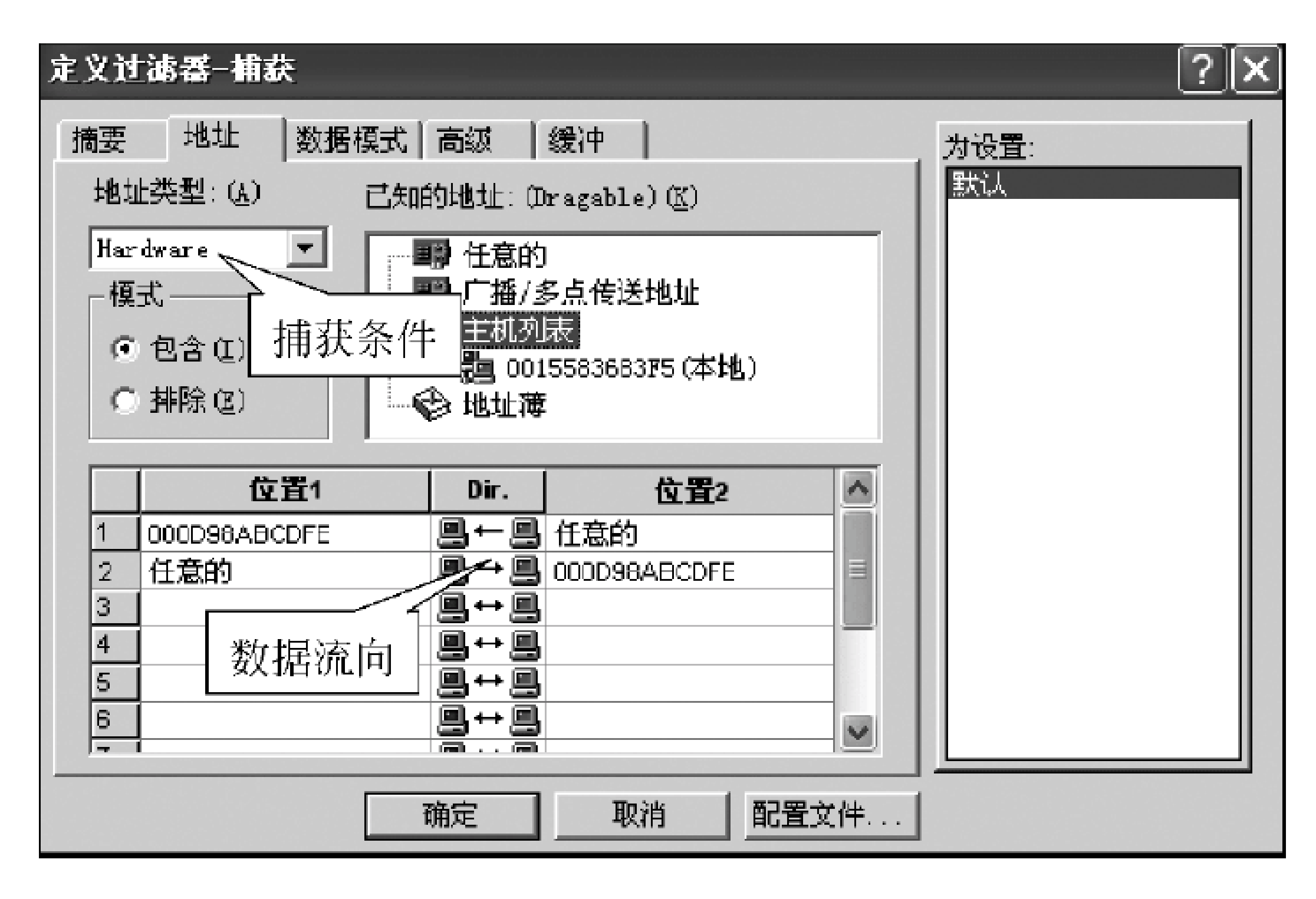


图 3.32　捕获条件定义界面

- 数据模式操作界面用来编辑捕获条件。
- 高级选项界面用来设定捕获的协议、数据包类型、数据包大小等信息。
- 缓冲操作界面用来对缓冲区进行详细配置。

在“高级”页面下，可以更加详细地配置捕获条件，如选择需要捕获的协议条件、数据包具体长度、数据包类型等。在保存过滤规则条件“配置文件(Profiles)”时，可以对当前设置的过滤规则进行保存，在捕获面板中，可以选择保存的捕获条件 默认 。

在“数据模式”页面下，可以编辑更加详细的捕获条件，如图 3.33 所示。利用数据模

式的方式可以实现复杂报文过滤，但同时增加了捕获的时间复杂度。

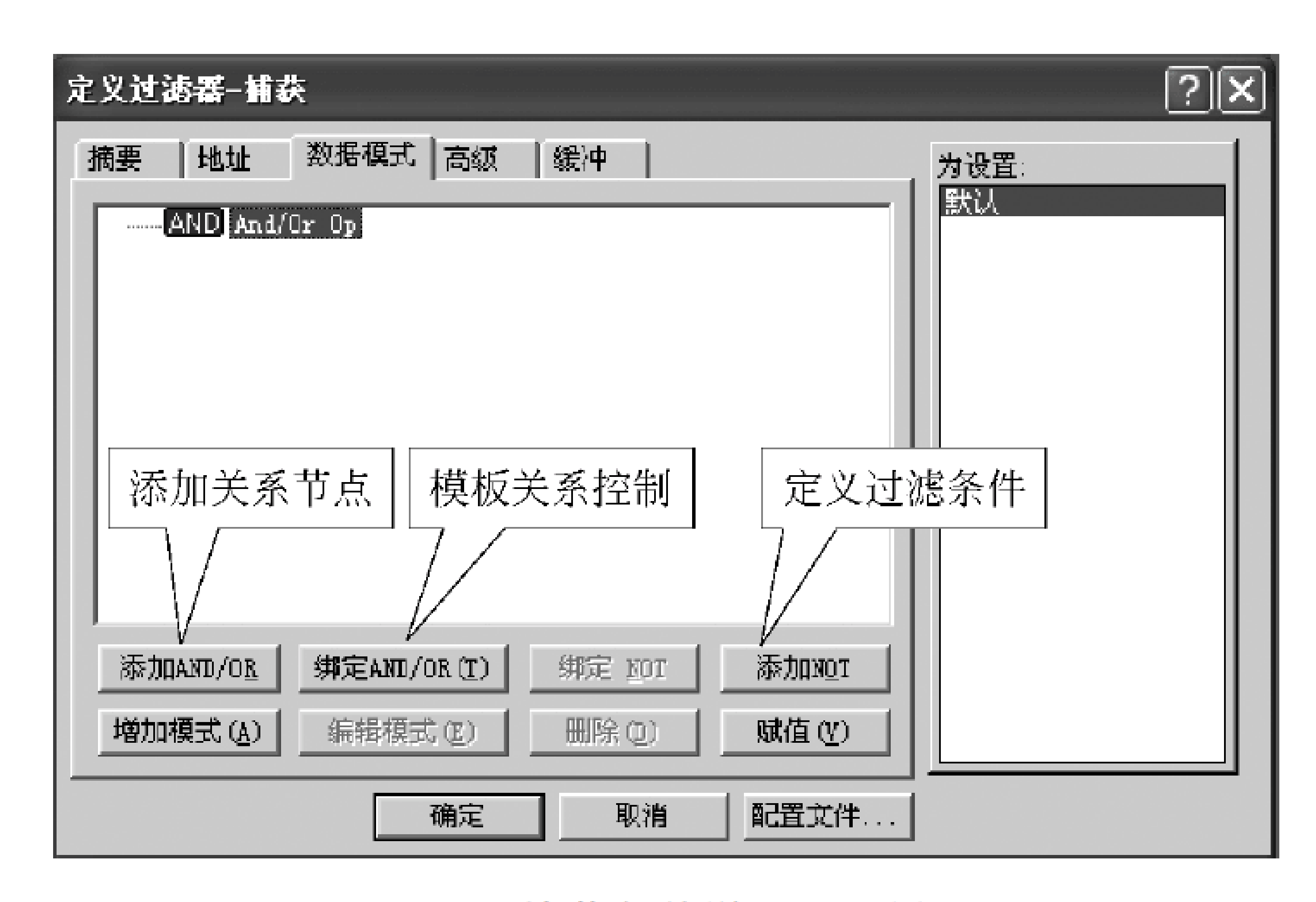


图 3.33 捕获条件详细配置界面

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

3.2.4 网络监视实验

实验器材

- Sniffer Pro 软件系统 1 套。
- PC(Windows XP/Windows 7)1 台。

预习要求

- 做好实验预习，复习网络协议有关内容。
- 复习 Sniffer 软件数据捕获功能的操作方法。
- 熟悉实验过程和基本操作流程。
- 做好预习报告。

实验任务

通过本实验，熟练掌握 Sniffer 的各项网络监视模块的使用；熟练运用网络监视功能，撰写网络动态运行报告。

实验环境

本实验采用一个已经连接并配置好的局域网环境。PC 上安装 Windows 操作系统。

预备知识

- TCP/IP 原理及基本协议。

- 数据交换技术概念及原理。
- 路由技术及实现方式。

实验步骤

单击“监视器”菜单或快捷操作界面，可依次看到如下监视功能：仪表板、主机列表、矩阵、请求响应时间、历史取样、协议分析、全局统计表、警报日志等。

1．仪表板（dashboard）

单击快捷操作菜单上的图标，即可弹出仪表板。在仪表板上方，可对监视行为进行具体配置，并对监视内容进行重置。如图 3.34 所示，网络监视仪表盘包括三个仪表：第一个仪表显示的是网络使用率（Utilization）；第二个仪表显示的是网络每秒钟通过的包数量（Packets）；第三个仪表显示的是网络的每秒错误率（Errors）。

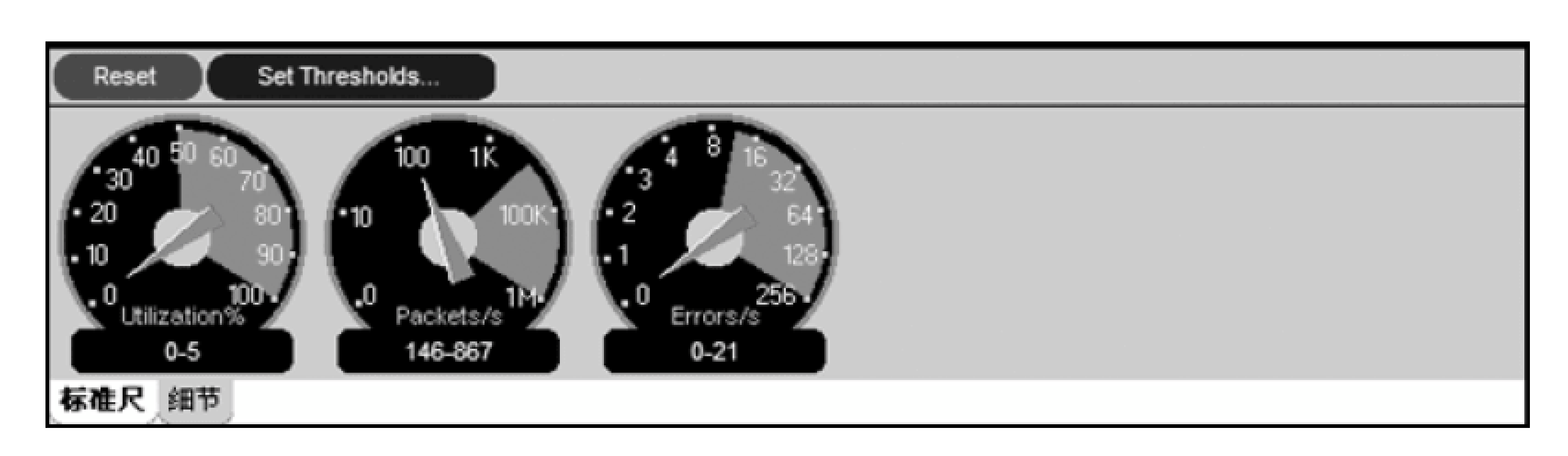


图 3.34　网络监视仪表信息

下面两组数字，前面表示当前值，后面表示最大值。通过三个仪表可以直观地观察到网络的使用情况，仪表的红色区域是警戒区域，如果发现有指针到了红色区域就该引起一定的重视了，说明网络线路不好或者网络负荷太大。如果需要获得更为详细的网络整体使用情况，可以单击“细节”按钮，查看数据统计结果。

如图 3.35 所示，Drops 表示网络中遗失的数据包数量（在网络活动高峰期经常会遗失数据包），过多的广播会使网络上所有系统的性能整体下降。在粒度分析表格中列出了网络中数据包的分布状态，包括 64B、65-127B、128-255B 等不同字节的数据包总数。错误描述表格中列出了错误出现率，也就是 Errors/s。

网络		粒度分布		错误描述	
数据包	340,768	64字节	23,074	CRCs	71
Drops	0	65-127字节	127,080	Runts	0
广播	5,360	128-255字节	23,328	太大的	0
多点传送	432	256-511字节	12,804	碎片	0
字节	232,901,272	512-1023字节	18,126	Jabbers	0
利用	0	1024-1518字节	136,356	队列	0
错误	71			Collisions	0

标准尺　细节

图 3.35　网络监视详细信息

通过三个仪表盘，可以很容易地看到从捕获开始，有多少数据包经过网络，有多少帧被过滤，以及遗失了多少帧等情况，还可以看到网络的利用率、数据包数目和广播数，如果发现网络在每天的特定时间都会收到大量的组播数据包，就说明网络可能出现了问题，需及时分析哪个应用程序在发送组播数据包。

Sniffer 的很多网络分析结果都可以设定阈值，若超出阈值，报警记录就会生成一条信息，并在仪表盘上以红色来标记阈值的警告值。网络管理员应记录下警告信息，并且查看系统超过了阈值多少次，以及超出阈值的频率是多少，这些信息有助于确定网络是否有问题。

单击仪表盘上的 Set Thresholds（设定阈值）按钮，打开 Dashboard Properties 对话框，即可根据自己的网络状况来配置仪表阈值，以保证仪表能准确地显示网络情况。

如图 3.36 所示，可以在仪表盘的下方查看网络监视曲线图，主要包括网络运行、错误率和粒度分布三种情况。Long Term 每 30 分钟采样一次，一共可以采样 24 小时；Short Term 每 30 秒采样一次，可以采样 25 分钟。

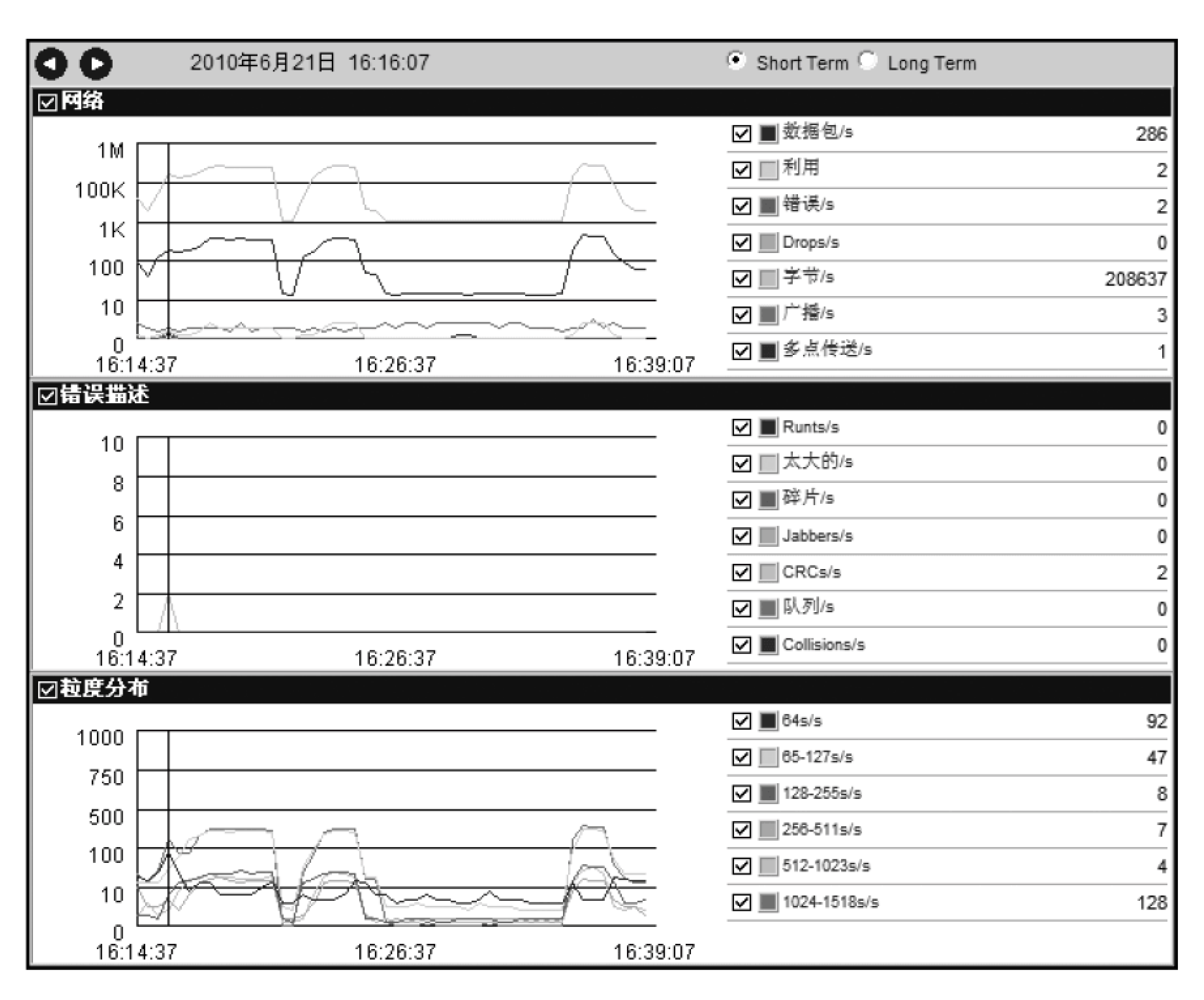


图 3.36 网络监视曲线图

2. 主机列表（host table）

单击快捷操作菜单上的图标，或选择“监视器”菜单内的“主机列表”选项，界面中显示的是所有在线的本网主机地址以及外网服务器地址信息，可以分别选择 MAC 地址、IP 地址以及 IPX 地址。通常情况下，网络中所有终端的对外数据，如浏览网站、上传下载等行为都是各终端与网关在数据链路层中进行的，因为需要查看 MAC 地址的连接情况。通过主机列表，可以直观地看到流量最大的前十位主机地址。

在查看网络主机信息时，默认以 MAC 地址形式显示网络中的计算机。如果计算机处于局域网中，可以清楚地显示计算机的 MAC 地址；但如果计算机处于 Internet 中，则不能获得计算机的 MAC 地址，此时以 IP 地址形式显示。单击窗口下方的 IP 标签，即可显示计算机的 IP 地址，这样可以更清楚地查看到各台计算机。

在列表中，可以通过单击“广播”或“多点传送”对广播量进行统计。IP 的广播有三种：255.255.255.255 叫本地广播；192.168.255.255 叫子网广播；192.168.1.255 叫全

子网广播。

为了方便查看连接地址信息,设置了细节、饼状图、柱状图等统计方式以及单向地址查看、输出、条件过滤等多种选项。在统计分析的柱形图与饼图中,网关流量依次减小。当发现某个网关流量与其他终端流量差距悬殊时,则需要重点检查目标主机是否有大网络流量的操作。如果发现某台计算机在某个时间段内发送或接收了大量数据,则说明其可能存在网络异常。

当选中某台主机时,可以通过“条件过滤”设置过滤条件,系统自动产生一个新的过滤器。在流量分析过程中,根据包结构取得主机信息,即目的 MAC、源 MAC 或目的 IP、源 IP。为了查看更为详细的主机交互情况,可以单击列表中的任意项,如图 3.37 所示,单击 IP 地址为“114.80.93.60”的列表项,则可以显示由“114.80.93.60”主机发送或接收的数据包情况,如图 3.38 所示。

Hw地址	入埠数据包	出埠数据包	字节	出埠字节	广播	多点传送	出埠错误	CRC	Jabbers	Runts	碎片	太大的
00016C8135AE	3	5	306	772	5	0	0	0	0	0	0	0
00016C8A758B	0	2	0	340	2	0	0	0	0	0	0	0
000C29E42021	0	1	0	247	1	0	0	0	0	0	0	0
000FE207F2E0	0	3	0	384	0	3	0	0	0	0	0	0
000FE2144E10	0	6	0	384	6	0	0	0	0	0	0	0
000FE2144EC0	0	6	0	384	6	0	0	0	0	0	0	0
000FE21C9F90	0	5	0	320	5	0	0	0	0	0	0	0
000FE25F3C8C	5,552	4,546	584,372	3,233,389	71	0	0	0	0	0	0	0
000FEAC30F6E	0	8	0	1,228	1	7	0	0	0	0	0	0
0013D3ACF6EA	0	1	0	253	1	0	0	0	0	0	0	0
0013D3C291DD	0	1	0	247	1	0	0	0	0	0	0	0
001558361 3DB	624	466	695,520	79,440	1	0	0	0	0	0	0	0
001558361430	19	20	3,824	2,122	0	0	0	0	0	0	0	0
0015605F328C	0	3	0	375	3	0	0	0	0	0	0	0
001560A1DD65	0	1	0	262	1	0	0	0	0	0	0	0
001560A5CA4D	0	1	0	64	1	0	0	0	0	0	0	0
0015F2D6D45D	0	526	0	50,496	526	0	0	0	0	0	0	0
0016353CB1A7	12	20	1,705	3,405	9	0	0	0	0	0	0	0
0016369E3C19	0	1	0	247	1	0	0	0	0	0	0	0
0016767D1E91	743	827	300,663	58,728	22	0	0	0	0	0	0	0
001A4B5C3C9B	0	20	0	2,063	16	4	0	0	0	0	0	0
001A4B81CFA0	0	1	0	64	1	0	0	0	0	0	0	0
001A92CC40EA	0	1	0	96	1	0	0	0	0	0	0	0
001BFC91049C	0	10	0	4,644	0	10	0	0	0	0	0	0
001E73965EA1	0	17	0	1,598	0	17	0	0	0	0	0	0
0050BF14DC64	0	5	0	1,165	5	0	0	0	0	0	0	0
00E04C3C2538	0	1	0	261	1	0	0	0	0	0	0	0
00E04CEEF8F5	0	347	0	29,734	347	0	0	0	0	0	0	0
01005E7FFFEF	6	0	396	0	0	0	0	0	0	0	0	0
01005E7FFFFA	10	0	5,322	0	0	0	0	0	0	0	0	0
0180C2000003	4	0	256	0	0	0	0	0	0	0	0	0
0180C200000A	3	0	384	0	0	0	0	0	0	0	0	0
02004C4F4F50	48	50	6,146	8,709	1	0	0	0	0	0	0	0
333300000005	17	0	1,598	0	0	0	0	0	0	0	0	0
3333FF965EA1	1	0	90	0	0	0	0	0	0	0	0	0
本地	3,056	4,249	2,224,669	442,192	16	0	0	0	0	0	0	0
广播	1,056	0	98,897	0	0	0	0	0	0	0	0	0
0014C254C5D0	0	1	0	64	1	0	0	0	0	0	0	0
002421EE8107	0	1	0	247	1	0	0	0	0	0	0	0
00016C8A6704	0	3	0	288	3	0	0	0	0	0	0	0

图 3.37 主机列表

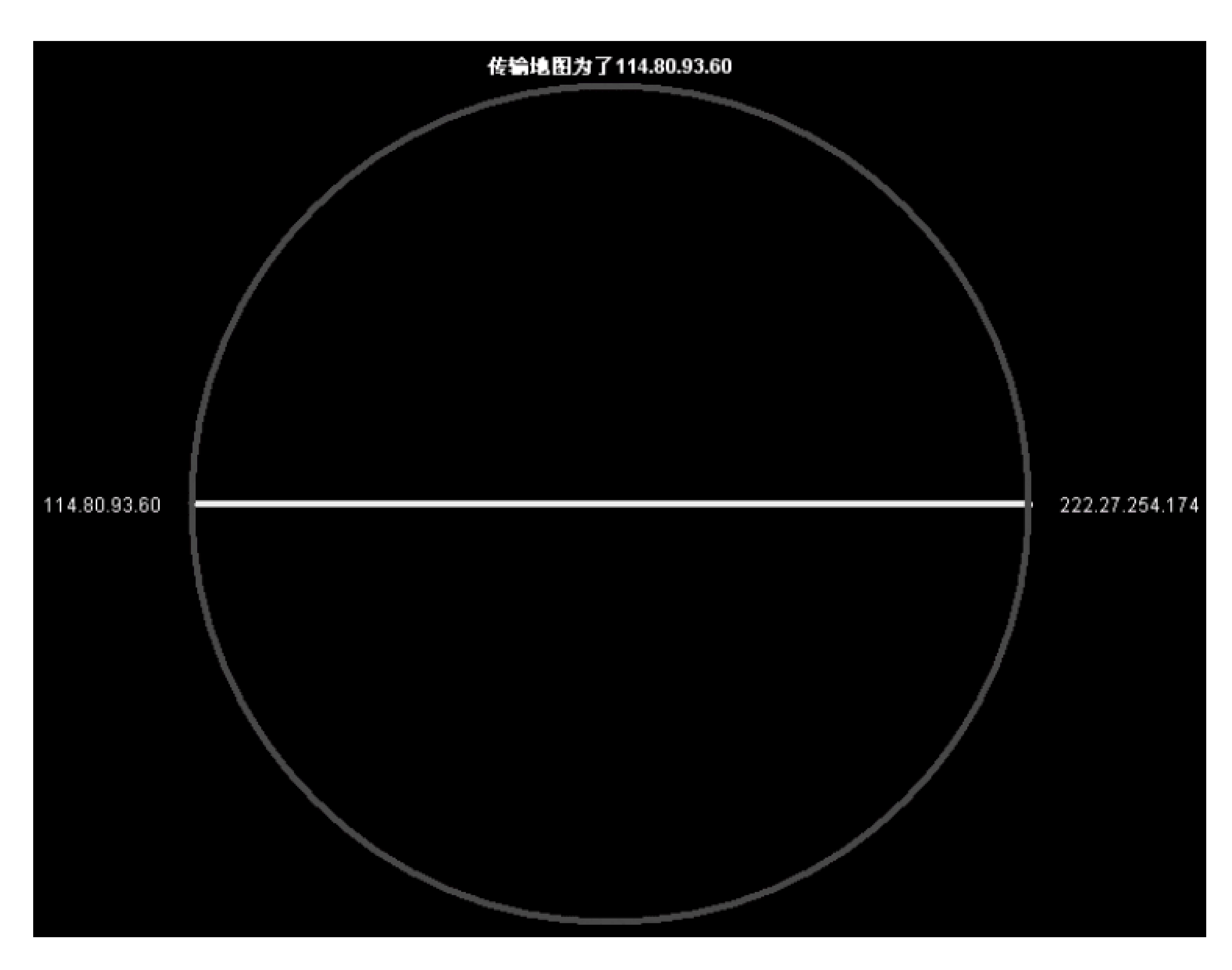


图 3.38 单机连接情况

3. 矩阵(matrix)

单击快捷操作菜单上的图标,或选择“监视器”菜单内的“矩阵”选项,可以显示全网的所有连接情况,即主机会话情况。

如图 3.39 所示,处于活动状态的网络连接被标记为绿色,已发生的网络连接被标记为蓝色,线条的粗细与流量的大小成正比,将鼠标移动至线条处,会显示流量双方位置、通信流量大小以及流量占当前网络的百分比。

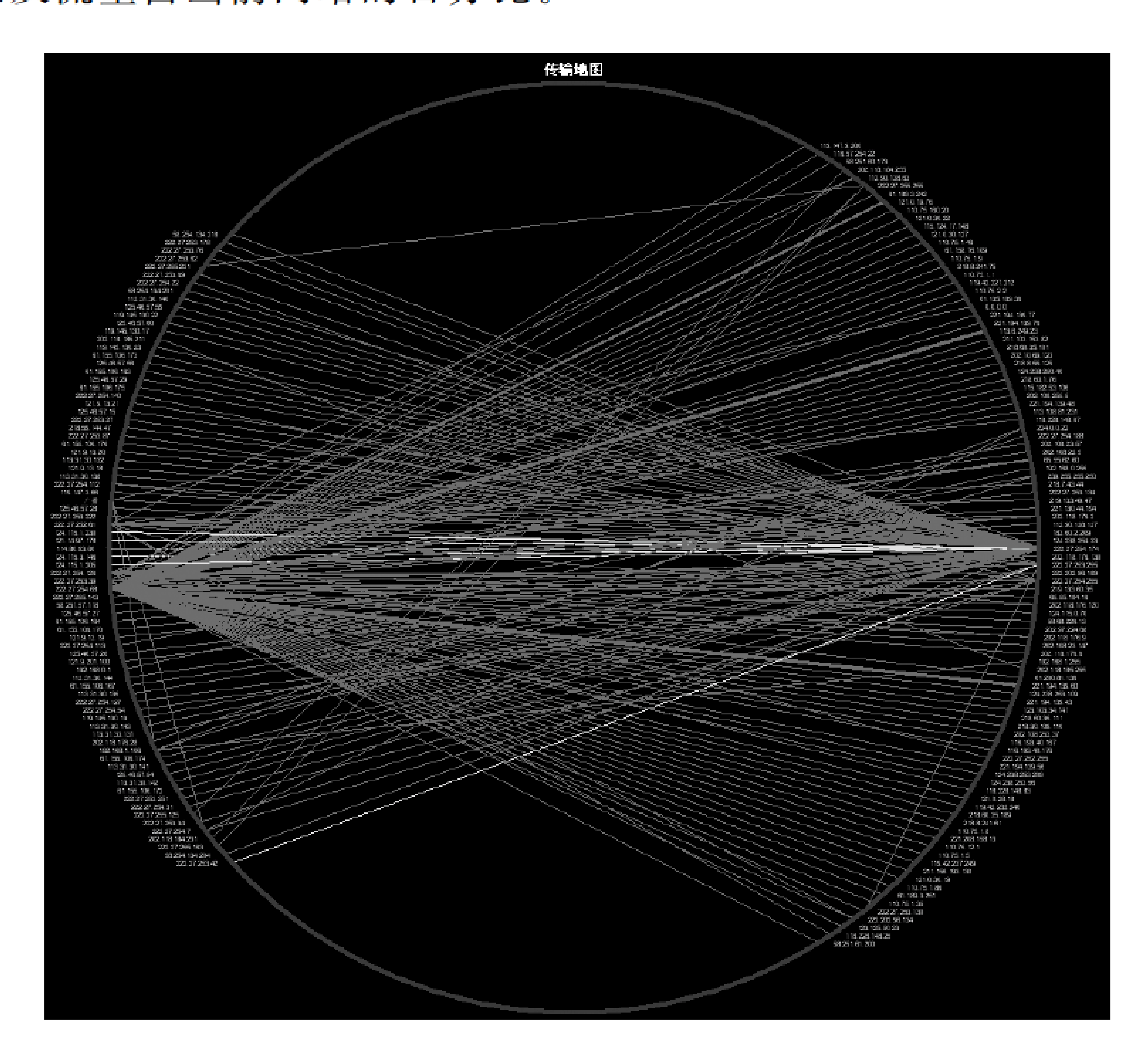


图 3.39　全网连接矩阵

- 对于 LAN,可以分析 MAC 层、IP 网络层、IP 应用层、IPX 网络层和 IPX 传输层。
- 对于 WAN,可以分析链路层、IP 网络层、IP 应用层、IPX 网络层和 IPX 传输层。

矩阵可以说是 Sniffer 中最常用的功能,它以矩阵方式列出当前网络中的连接情况,用户可以清楚地看到某个计算机正在与哪些地址进行连接。

“通信量图”可以显示节点间网络通信量的全面信息,而且可以查看特定网络节点信息。

“大纲”简要汇总了每对网络节点间发送的总字节数和总报文数,可以查看独立网络连接的数据包使用情况,也可以右击独立的 IP 终端节点,如果连接数目非常大,显然不是一种正常的业务连接,此时需要认真检查每一个连接的会话情况。

如图 3.40 所示,细节可以按高层协议分类情况查看网络连接及数据包使用情况。此外,柱状图以及饼图都能够实时显示网络利用率在前十位的网络连接会话。利用矩阵监视器可以评估网络运行状况和流量异常,特别适合用来检测病毒。

对于未知协议,可以通过选择“工具”菜单的“设置”选项下的“协议”栏进行自定义,为某端口指定协议名称,以便更好地检测网络流量。

通过矩阵功能可以发现网络中使用 BT 等 P2P 软件或中了蠕虫病毒的用户。如果某

协议	主机1	数据包	字节	字节	数据包	主机2
Bootpc	192.168.1.106	4	1,384	0	0	广播
	0.0.0.0	2	732	0	0	
DNS	222.27.252.61	3	250	573	3	202.118.176.2
	222.27.254.68	1	74	149	1	
	222.27.253.39	2	167	709	2	
	222.27.254.174	3	244	640	3	
	222.27.254.126	19	1,539	4,936	19	
	222.27.254.68	68	5,473	17,644	68	202.97.224.68
	222.27.252.61	1	417	64	1	124.238.254.33
HTTP	222.27.254.126	7	801	5,554	7	113.108.81.231
	222.27.254.68	53	7,844	20,023	40	202.108.255.5
		6	923	2,800	6	121.0.28.18
		6	644	758	6	124.238.253.109
	222.27.254.126	15	1,494	2,388	15	61.135.189.36
	222.27.254.68	20	3,646	3,940	20	110.75.2.2
		7	713	8,410	8	221.194.139.48
	222.27.254.126	25	3,110	3,545	25	118.228.148.83
	222.27.254.68	25	7,628	3,513	25	119.42.233.240
		10	1,646	1,252	10	202.108.23.57
		10	1,390	858	10	202.108.23.147
		122	15,683	129,561	137	218.8.241.61
		9	1,305	11,762	12	110.75.1.1
		175	18,785	307,426	243	221.194.139.43
		175	14,465	281,607	225	218.60.35.189
		416	179,268	369,317	465	202.118.176.9
		9	2,357	667	5	124.238.253.56
		12	1,493	9,965	14	202.108.22.5
		11	2,077	4,907	11	119.42.227.212
		12	2,053	7,463	10	221.194.139.77
		16	2,663	13,123	15	124.238.253.209
		93	13,174	122,150	114	221.194.139.76
		6	806	1,207	5	218.30.109.110
		709	136,352	1,095,430	880	221.194.139.60
		5	795	359	3	218.8.55.125
	222.27.252.61	10	1,733	1,266	10	118.228.148.67
	222.27.254.68	22	2,905	12,022	21	218.60.35.111
	61.200.81.136	32	36,896	3,372	34	222.27.254.126
	222.27.254.68	23	1,998	39,371	31	124.238.250.40
		6	820	2,274	6	202.108.253.37
		16	2,795	4,880	8	202.10.69.120
		9	1,311	3,813	8	116.193.40.167
		78	17,712	56,647	83	202.118.176.6
		5	697	1,171	3	221.194.139.56
		80	9,629	98,249	100	218.8.241.75
		10	1,246	2,346	10	211.103.153.82

图 3.40　不同网络协议的网络连接情况

个用户的并发连接数特别多,并且在不断地向其他计算机发送数据,这就说明该计算机很可能中了蠕虫等病毒。此时,网络管理员应及时封掉该计算机所连接的交换机端口,并对该计算机查杀病毒。

4. 请求响应时间(application response time,ART)

请求响应时间用来显示网络中 Web 网站的连接情况,可以看到局域网中有哪些计算机正在上网,浏览的是哪些网站等。该窗口中显示了局域网内的通信及数据传输大小,并且显示了本地计算机与 Web 网站的 IP 地址。通过单击左侧工具栏中的图标,以柱形图方式显示网络中计算机的数据传输情况,不同顺序图柱代表右侧列表中的相应连接,柱形长短表示传输量的大小。

ART 是指一个客户端发出一个请求,到服务器响应回来的时间差。一般来说,应用响应的快慢是应用性能的一个重要指标。应用性能主要取决于几个因素:网络因素、服务器因素、客户端因素、应用协议因素。

如果一个数据包的目的 IP 是 192.168.1.1,目的端口是 80,那么就可以认定 192.168.1.1 是 Http 服务器地址,而源 IP 就是客户地址,主要列表项含义如图 3.41 所示。

服务器地址	客户地址	AvgRsp	90%Rsp	MinRsp	MaxRsp	TotRsp	0-25	26-50	51-100	101-200	201-400	401-800	301-66	服务器Octe..	客户Octets	重试	超时设...
110.76.33.15	222.27.252.61	67	66	67	68	3	0	0	3	0	0	0	0	8,501	847	0	0
112.90.137.39	525F2149DE724FF	62	61	62	62	3	0	0	3	0	0	0	0	8,795	755	0	0
113.6.254.49	525F2149DE724FF	3	2	1	5	18	18	0	0	0	0	0	0	5,806	3,727	0	0
113.6.254.6	525F2149DE724FF	2	2	1	4	13	13	0	0	0	0	0	0	10,514	3,273	1	1
118.144.78.38	525F2149DE724FF	31	41	24	43	13	1	12	0	0	0	0	0	585K	4,233	0	0
118.228.148.67	222.27.252.61	18	16	17	20	4	4	0	0	0	0	0	0	1,266	1,349	0	0
c25-zol-pv-web-80.	222.27.253.125	26	28	24	28	11	4	7	0	0	0	0	0	4,577	7,172	0	0
c25-zol-active-web	222.27.253.125	28	28	28	28	3	0	3	0	0	0	0	0	764	1,366	0	0
c25-dw-xw-lb.cnet.	222.27.253.125	27	27	26	27	4	0	4	0	0	0	0	0	1,596	3,234	0	0
c25-zol-detail-web-	222.27.253.125	32	49	28	57	15	0	14	1	0	0	0	0	64,407	9,878	0	0
c25-zol-pic-web-80	222.27.253.125	27	29	25	29	54	0	54	0	0	0	0	0	398K	24,525	0	0
119.147.18.8	222.27.252.61	160	155	158	161	2	0	0	0	2	0	0	0	1,714	441	0	0
122.141.225.13	525F2149DE724FF	45	43	45	46	2	0	2	0	0	0	0	0	34,657	294	0	0
122.224.95.187	222.27.253.125	65	80	54	84	6	0	0	6	0	0	0	0	5,333	2,863	0	0
123.138.238.206	525F2149DE724FF	44	43	44	45	2	0	2	0	0	0	0	0	517	845	0	0
lvs1.bmvip.cnz.alim	222.27.252.61	50	50	49	50	2	0	1	1	0	0	0	0	13,902	591	0	0
ydt.lzs.vip.cnz.alim	222.27.252.61	44	42	44	44	2	0	2	0	0	0	0	0	881	1,513	0	0
121.194.1.101	222.27.252.61	16	15	16	17	2	2	0	0	0	0	0	0	4,281	480	0	0
acookie1.taobao.v	222.27.252.61	62	62	62	63	2	0	0	2	0	0	0	0	787	1,093	0	0
p4.mm.vip.cnz.alim	222.27.252.61	50	50	49	50	4	0	1	3	0	0	0	0	4,050	2,232	0	0
121.194.7.169	222.27.252.61	16	15	16	17	2	2	0	0	0	0	0	0	526	1,050	0	0
123.138.238.204	222.27.253.142	44	42	44	44	2	0	2	0	0	0	0	0	517	920	0	0
124.238.253.109	525F2149DE724FF	95	90	95	95	2	0	0	2	0	0	0	0	758	388	0	0
124.238.254.32	222.27.252.61	134	164	87	180	2	0	0	1	1	0	0	0	432	1,296	0	0
124.238.254.94	222.27.253.125	104	105	104	105	6	0	0	0	6	0	0	0	2,076	2,456	0	0
124.89.103.101	525F2149DE724FF	80	77	79	80	2	0	0	2	0	0	0	0	14,741	367	0	0
124.89.30.138	525F2149DE724FF	81	78	80	81	2	0	0	2	0	0	0	0	689	317	0	0
125.211.213.130	222.27.253.142	2	2	1	3	20	20	0	0	0	0	0	0	7,390	2,100	0	0
125.39.127.25	525F2149DE724FF	73	71	72	73	2	0	0	2	0	0	0	0	7,123	683	0	0
125.39.127.25	222.27.253.142	44	42	44	44	2	0	2	0	0	0	0	0	24,568	724	0	0

图 3.41　ART 监视功能图

- AvgRsp：平均响应时间。
- 90%Rsp：90%响应时间，去掉头尾各 5%。
- MinRsp/MaxRsp：最大/最小的响应时间，以毫秒为单位。
- TotalRsp：响应次数。

接下来各列为 0～25ms 的响应次数，25～50ms 的响应次数等。

通过单击左侧的"属性"项，自定义所要监视的网络协议。当协议不存在时，可以利用对应端口号在"工具"菜单的"选项"对话框下添加协议。

利用应用响应时间的监视功能，可以快速获得某一业务的响应时间。首先获得业务源地址的服务器/客户端响应时间（网络消耗时间）和服务器处理时间；同时，在业务的目的地址获得服务器处理时间，利用 Sniffer 可以判断影响业务性能的因素是来自网络还是服务器。通过长期的观测，还可以设定每一个业务的响应基准线，以此判断业务运行是否正常。

5. 历史取样（history sample）

历史取样用来收集一段时间内的各种网络流量信息。通过这些信息可以建立网络运行状态基线，设置网络异常的报警阈值。默认情况下，历史采样的缓冲有 3600 个采样点，每隔 15 秒进行一次采样，采样 15 个小时后自动停止。如果想延长采样时间，可以通过修改采样间隔时间或者设置缓冲区属性的方式。具体做法是：单击左侧的"属性"按钮，修改采样间隔，并选中"当缓冲区满时覆盖"选项。此外，还可以灵活地选择多种采样项目。

6. 协议分布（protocol distribution）

协议分布用来分析网络中不同协议的使用情况。通过协议分布功能可以直观地看到当前网络流量中的协议分布情况，了解各类网络协议的分布情况以后，可以找到网络中流量最大的主机，这意味着该主机对网络的影响最大，之后可以利用主机列表的饼视图功能找到流量最大的机器。

7. 全局统计表

全局统计数据能够显示网络的总体活动情况，并确认各类数据包通信负载大小，从而

分析网络的总体性能及存在的问题。全局统计表提供了与网络流量相关的各类统计测量方式。

- 粒度分布：根据数据包大小与监测到的通信总量之比，显示每个数据包的发生频率。
- 利用率分布：以10%为基本度量单位，显示每组空间内网络带宽的分布情况。

8. 警报日志

全面监测和记录网络异常事件。一旦超过用户设定的阈值参数，警报器会在警报日志中记录相应事件。警报分为五种不同程度的严重性级别：严重、重要、次要、警告和通知。对于警报日志中的每个警报事件，都可以观察触发警报的具体节点类型、发生时间、警报级别以及描述信息等。系统默认的警报级别如表3.3所示。

表3.3　系统默认警报级别

事件	级别	事件	级别
阈值超过上限	严重	地址簿内数据重复	通知
IP地址重复	严重	探测位置不响应	次要

选择“工具”菜单中的“选项”，单击“警报”选项卡，选择“定义强度...”，可以修改警报强度，如图3.42所示。警报可以设定为声音、电子邮件、拨呼叫器以及警报文本四类。



图3.42　警报级别调整界面

同时，可以对专家系统的实时分析数据设定警报级别。选择“工具”下的“专家系统”选项，单击“警报”选项卡，将设定好严重性级别的各类系统层项目的“记录警报”选项设定为“是”。在正常运行过程中，选中“警报”选项卡上的“启用新警报”复选框即可。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

3.3 扩展实验

为了对 Sniffer Pro 的使用有一个更加综合和全面的了解,设计了网络协议嗅探和协议抓包分析两个综合型实验。

3.3.1 网络协议嗅探

实验器材

- Sniffer Pro 软件系统 1 套。
- PC(Windows XP/Windows 7)1 台。

预习要求

- 做好实验预习,复习网络协议有关内容。
- 复习 Sniffer 软件的操作方法。
- 熟悉实验过程和基本操作流程。
- 做好预习报告。

实验任务

通过本实验,理解常用 Sniffer 工具的配置方法,明确多数相关协议的明文传输问题;理解 TCP/IP 主要协议的报头结构,掌握 TCP/IP 网络的安全风险。

实验环境

本实验采用一个已经连接并配置好的局域网环境。PC 上安装 Windows 操作系统。

预备知识

- TCP/IP 原理及基本协议。
- FTP 站点搭建技术及基本协议。

实验步骤

1. 开启 Sniffer Pro

具体操作步骤略。

2. 捕获数据包前的准备工作

在默认情况下,Sniffer 将捕获其接入网络中的所有数据包,但在某些场景下,有些数据包可能不是我们所需要的,为了快速定位网络问题所在,有必要对所要捕获的数据包进行过滤。可以通过过滤器,定义 Sniffer 捕获数据包的过滤规则,过滤规则包括网络地址的定义和几百种协议的定义。定义过滤规则的做法如下:

在主界面选择"捕获"菜单中的"定义过滤器"选项,如图 3.43 所示。

其中,"地址"选项卡是最常用的过滤手段,包括 MAC 地址、IP 地址和 IPX 地址的过滤定义。以定义 IP 地址过滤为例,如图 3.44 所示。

当需要捕获地址为 192.168.1.224 的主机与其他主机数据通信时,需要首先确定"地

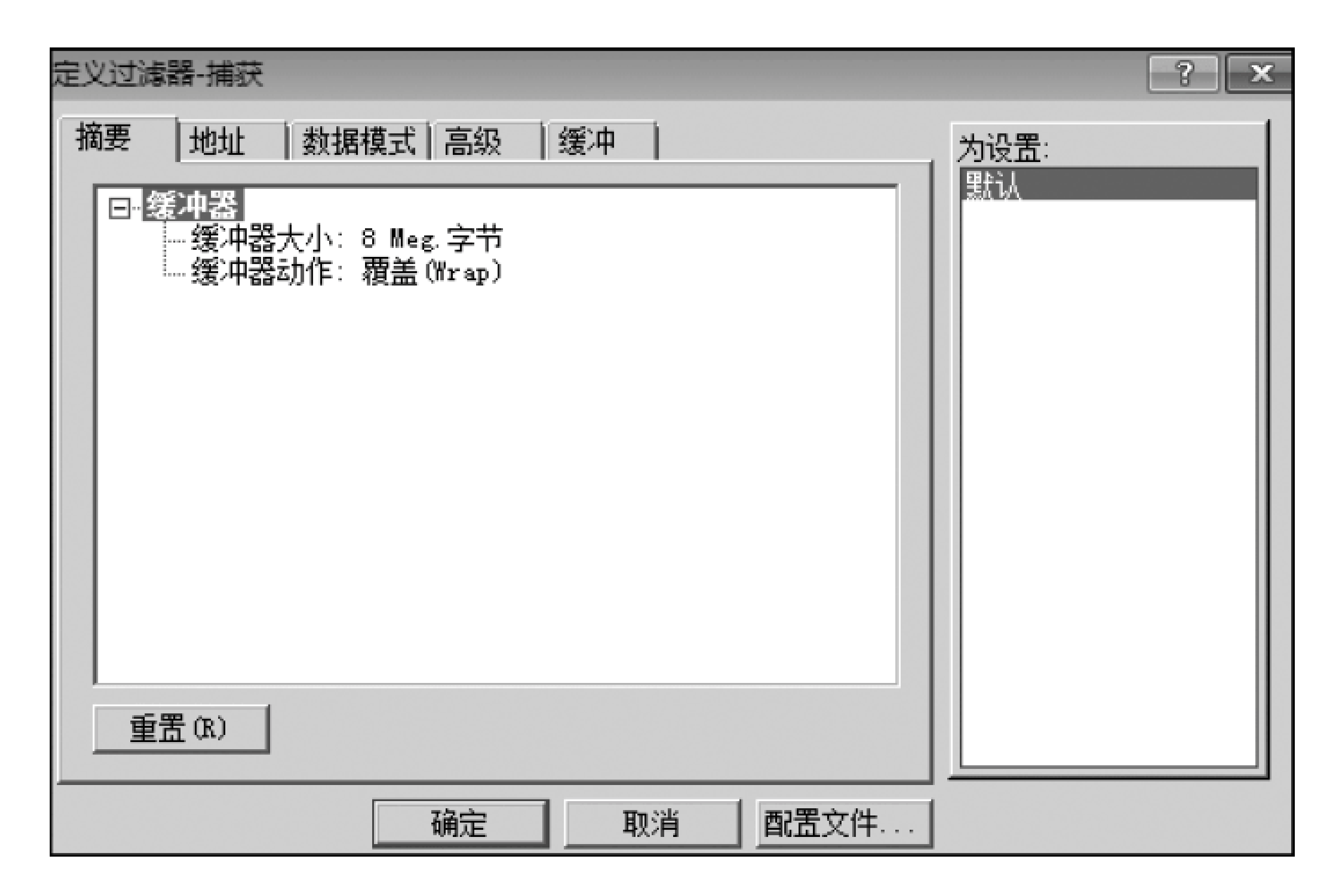


图 3.43 过滤器设定界面



图 3.44 IP地址过滤设定界面

址类型”为“IP”,“模式”为“包含”,若选择“排除”,则表示捕获条件为除本主机以外的所有数据通信。在下方的位置选项中,在左右任意一侧填写好主机地址,即“192.168.1.224”,而另一侧可填写“any”,完成通信地址定义。

- ↔ 表示由被测主机发出和接收的所有数据包。
- → 表示由被测主机发送的数据包。
- ← 表示由被测主机接收的数据包。

在完成上述设置后,要按照需要捕获的数据包类型选择可用协议,如 HTTP、DNS 等,需要特别注意的是,DNS、NETBIOS 的数据包有些是属于 UDP 协议,因此,需要在 UDP 选项卡中进行类似 TCP 选项卡的选择工作,否则捕获的数据包将不完整。

在“高级”设置栏目内,可以定义数据包大小(68～128B)、缓冲区大小以及文件存放位置等,具体内容如图 3.45 所示。

3. 捕获数据协议

将定义好的过滤器应用于捕获操作中。启动“捕获”功能,就可以运用各种网络监控功能分析网络数据流量及各种数据包具体情况。



图 3.45　协议过滤设定界面

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

3.3.2　FTP 协议分析

实验器材

- Sniffer Pro 软件系统 1 套。
- PC(Windows XP/Windows 7)1 台。

预习要求

- 做好实验预习,复习网络协议有关内容。
- 复习 Sniffer 软件的操作方法。
- 熟悉实验过程和基本操作流程。
- 做好预习报告。

实验任务

通过本实验,掌握利用 Sniffer 软件捕获和分析网络协议的具体方法。

实验环境

本实验采用一个已经连接并配置好的局域网环境。PC 上安装 Windows 操作系统。

预备知识

- FTP 原理及基本协议。
- 网络协议分析技术的综合运用。

实验步骤

按照实际需要，定义如图 3.46 所示的过滤器，并应用该过滤器捕获 FTP 协议信息。运行数据包捕获功能。

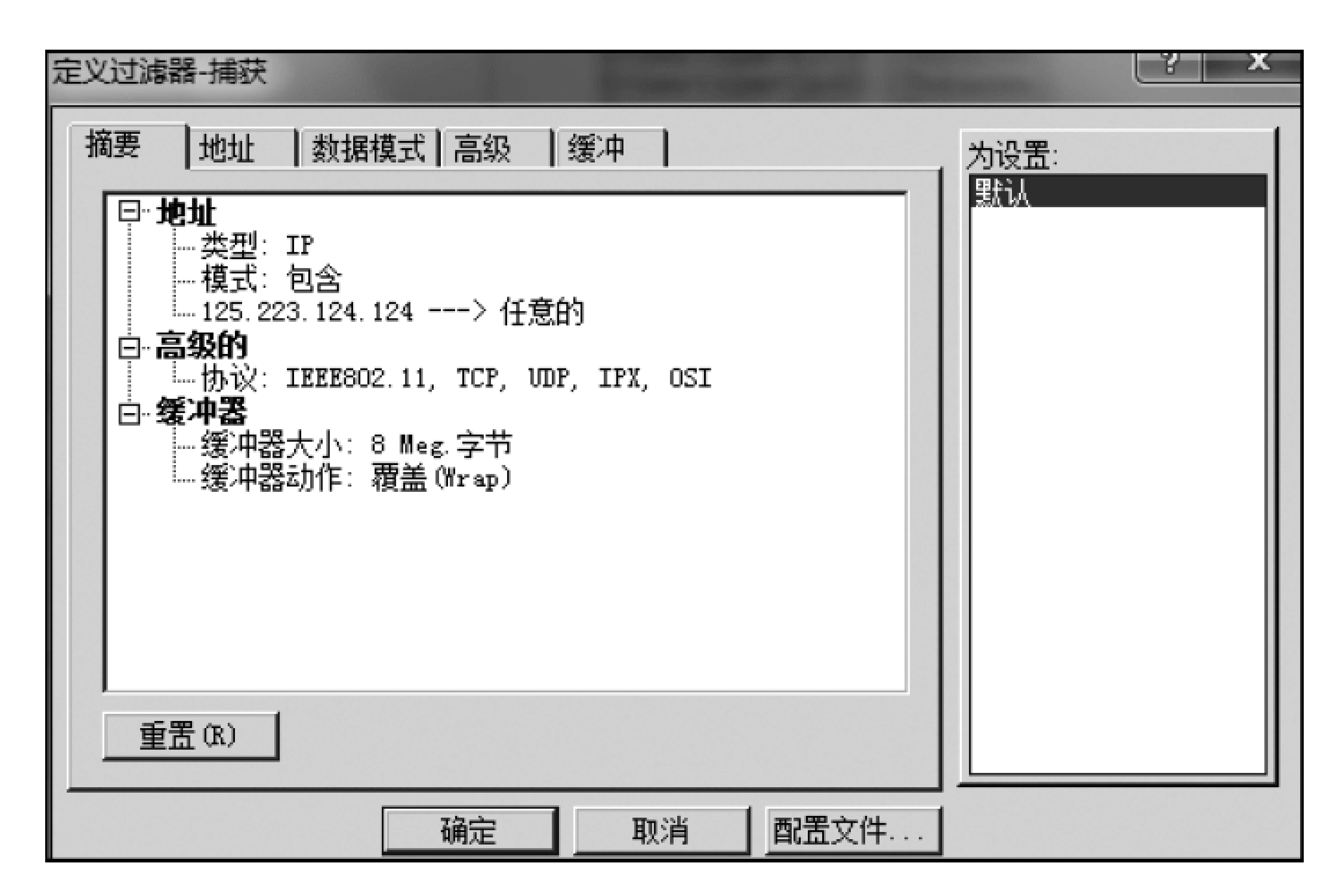


图 3.46　定义过滤器

在 Sniffer 捕获状态下，进行 FTP 站点操作。如图 3.47 所示，登录 FTP 站点，位置信息为“ftp. hrbeu. edu. cn”，用户名和密码均为匿名(anonymous)。看到系统登录成功的提示后，用户可以进行自定义操作，对 FTP 站点和文件进行操作。

```
C:\Windows\system32\cmd.exe - ftp  ftp.hrbeu.edu.cn
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\sunjianguo>ftp ftp.hrbeu.edu.cn
连接到 ftp2007.hrbeu.edu.cn。
220 (vsFTPd 2.0.5)
用户(ftp2007.hrbeu.edu.cn:(none)): anonymous
331 Please specify the password.
密码:
230 Login successful.
ftp> list
无效命令。
ftp>
```

图 3.47　FTP 命令行登录界面

通过单击“捕获停止”或者“停止并显示”按钮停止 Sniffer 捕获操作，并对捕获的数据包进行解码和显示。如图 3.48 所示，通过对报文解析，可以看到 Sniffer 捕获到了用户登录 FTP 的用户名和明文密码，对于用户进行的若干 FTP 站点操作行为，Sniffer 都能够捕获到相关信息。

实验报告要求

- 实验目的。

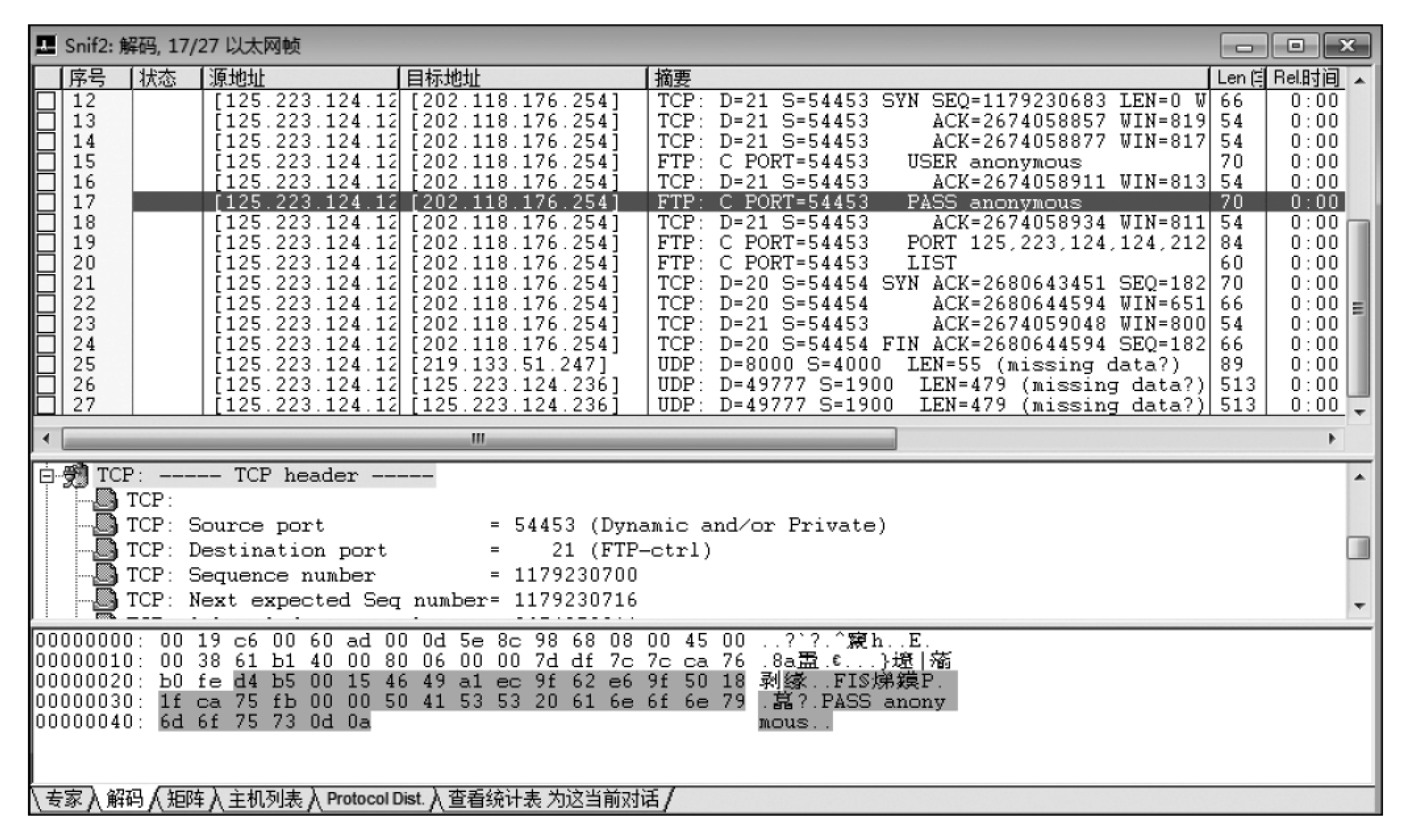


图 3.48 FTP命令行登录界面

- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

3.3.3 Telnet 协议分析

实验器材

- Sniffer Pro 软件系统 1 套。
- PC(Windows XP/Windows 7)1 台。

预习要求

- 做好实验预习,复习网络协议有关内容。
- 复习 Sniffer 软件的操作方法。
- 熟悉实验过程和基本操作流程。
- 做好预习报告。

实验任务

通过本实验,掌握利用 Sniffer 软件捕获和分析网络协议的具体方法。

实验环境

本实验采用一个已经连接并配置好的局域网环境。PC 上安装 Windows 操作系统。

预备知识

- Telnet 原理及基本协议。
- 网络协议分析技术的综合运用。

实验步骤

按照实际需要，定义如图 3.49 所示的过滤器，并应用该过滤器捕获 Telnet 协议信息。运行数据包捕获功能。

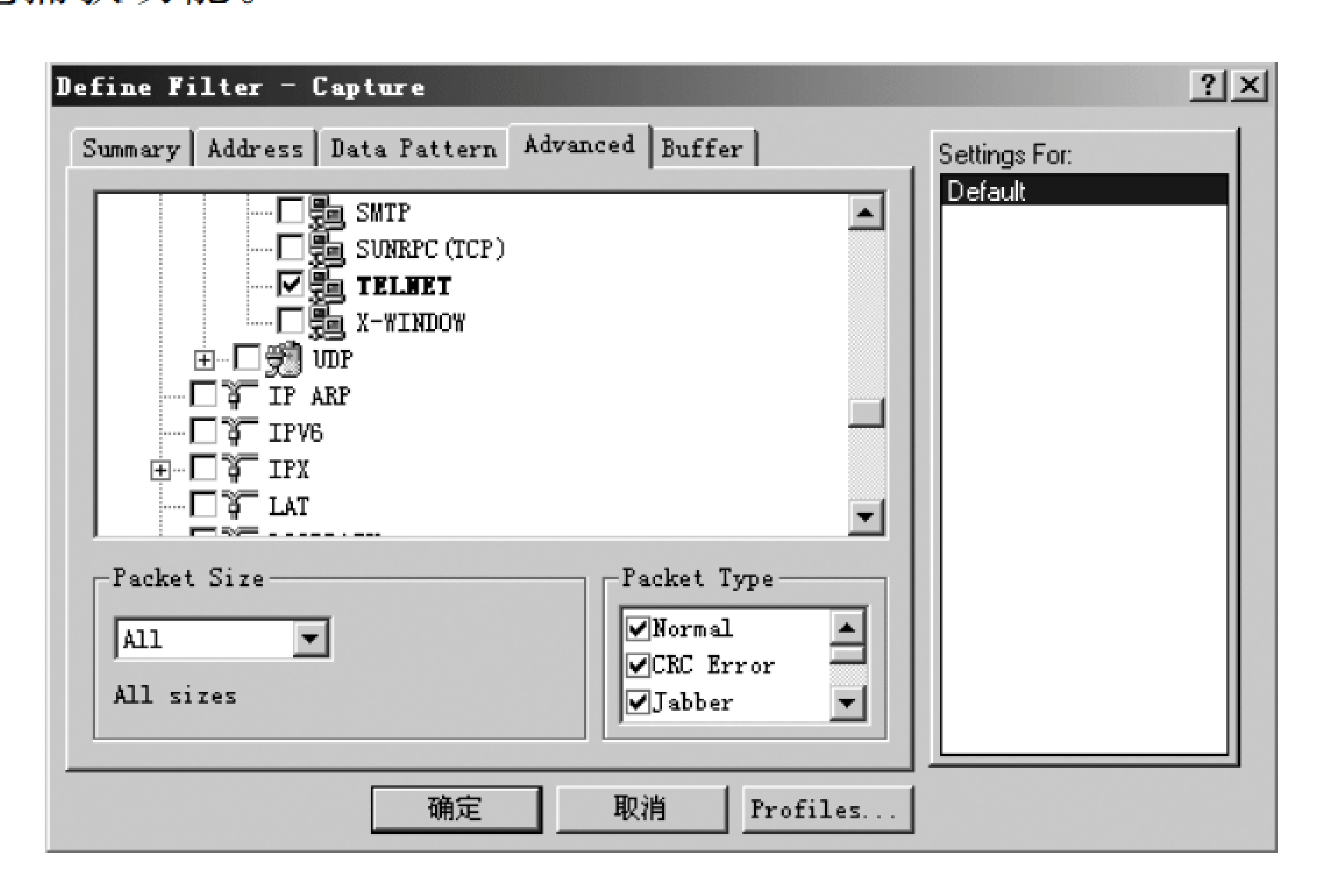


图 3.49　定义 Telent 协议的过滤器

在应用 Telnet 方式登录远程计算机之前，需要开启 Telent 服务。如果计算机安装的是 Windows 7 操作系统，则需要单独下载 TELNET.exe 程序。在登录远程计算机时，需要知道该计算机的用户名和密码。

有关该项目的测试，可以选择在局域网内进行分组练习，两人一组，分别 Telnet 到对方计算机。如图 3.50 和图 3.51 所示。

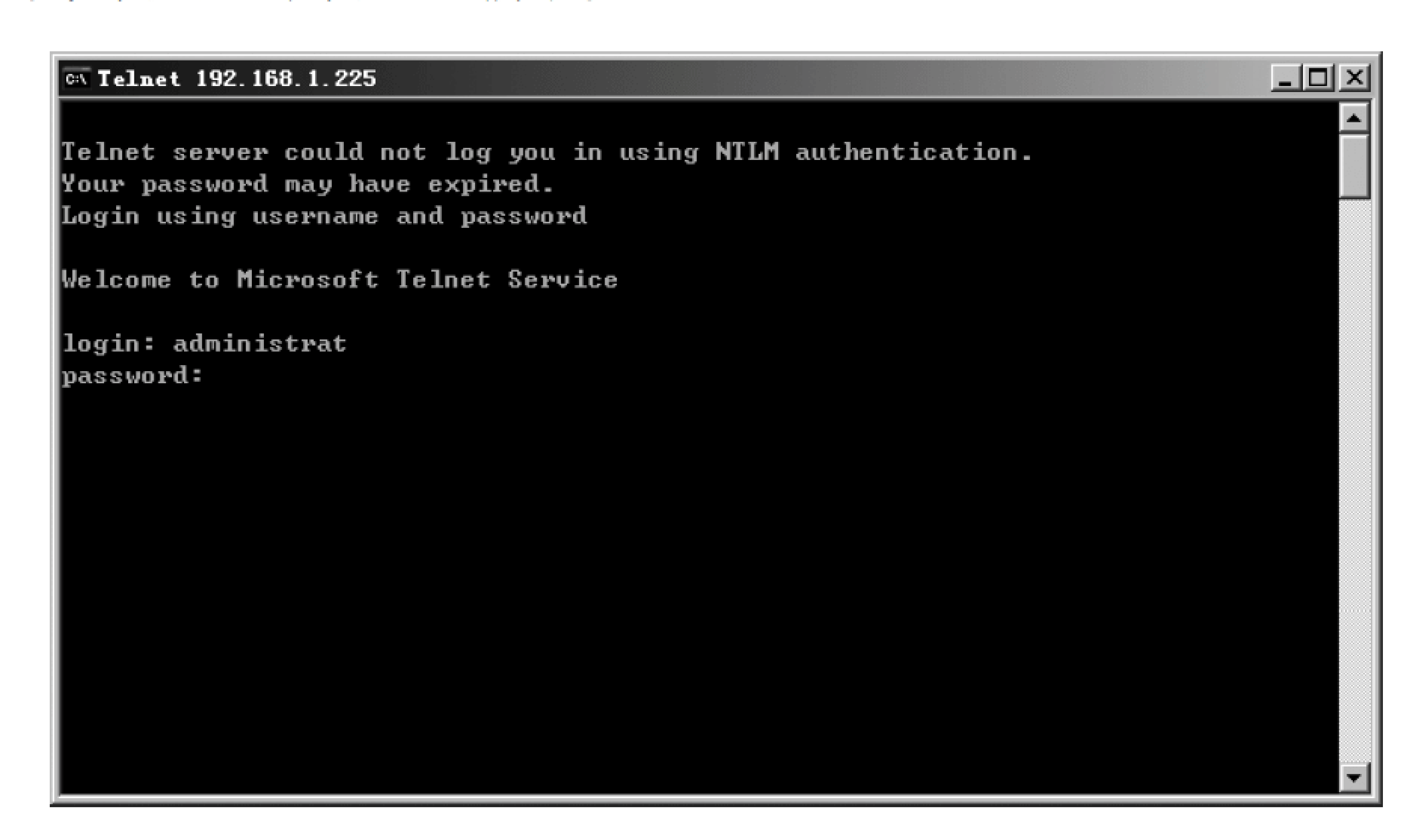


图 3.50　远程登录界面

由于 Telnet 登录时口令部分不回显，只能抓取从 Client 到 Server 的报文才能获取明文口令，所以一般嗅探软件无法直接看到口令。默认情况下，Telnet 登录时进入字符输入模式，而非行输入模式，此时基本上是客户端一有击键就立即向服务器发送字符，TCP 数据区就存储一个字节。如图 3.52 所示为嗅探的结果。

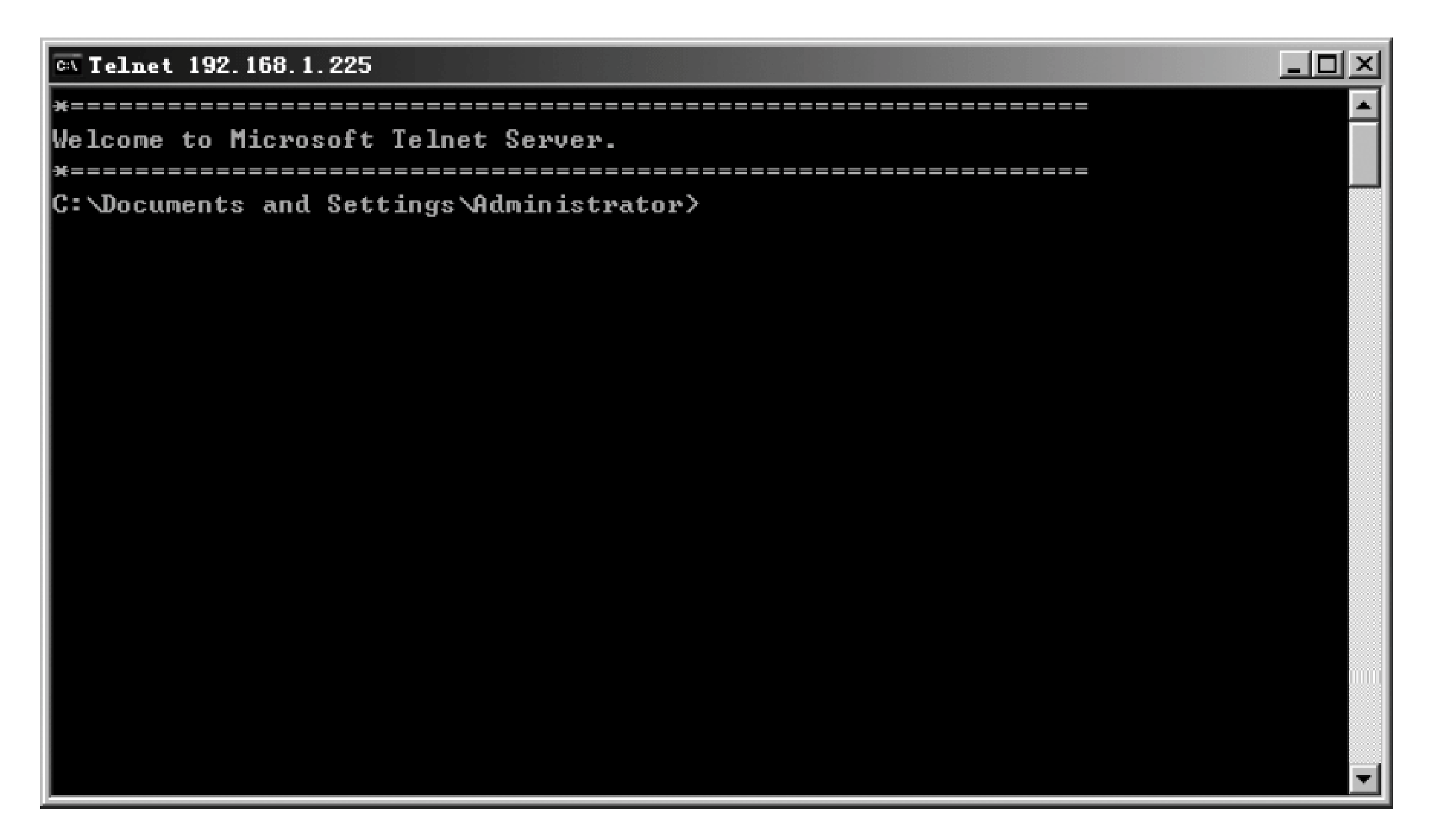


图 3.51　远程连接成功

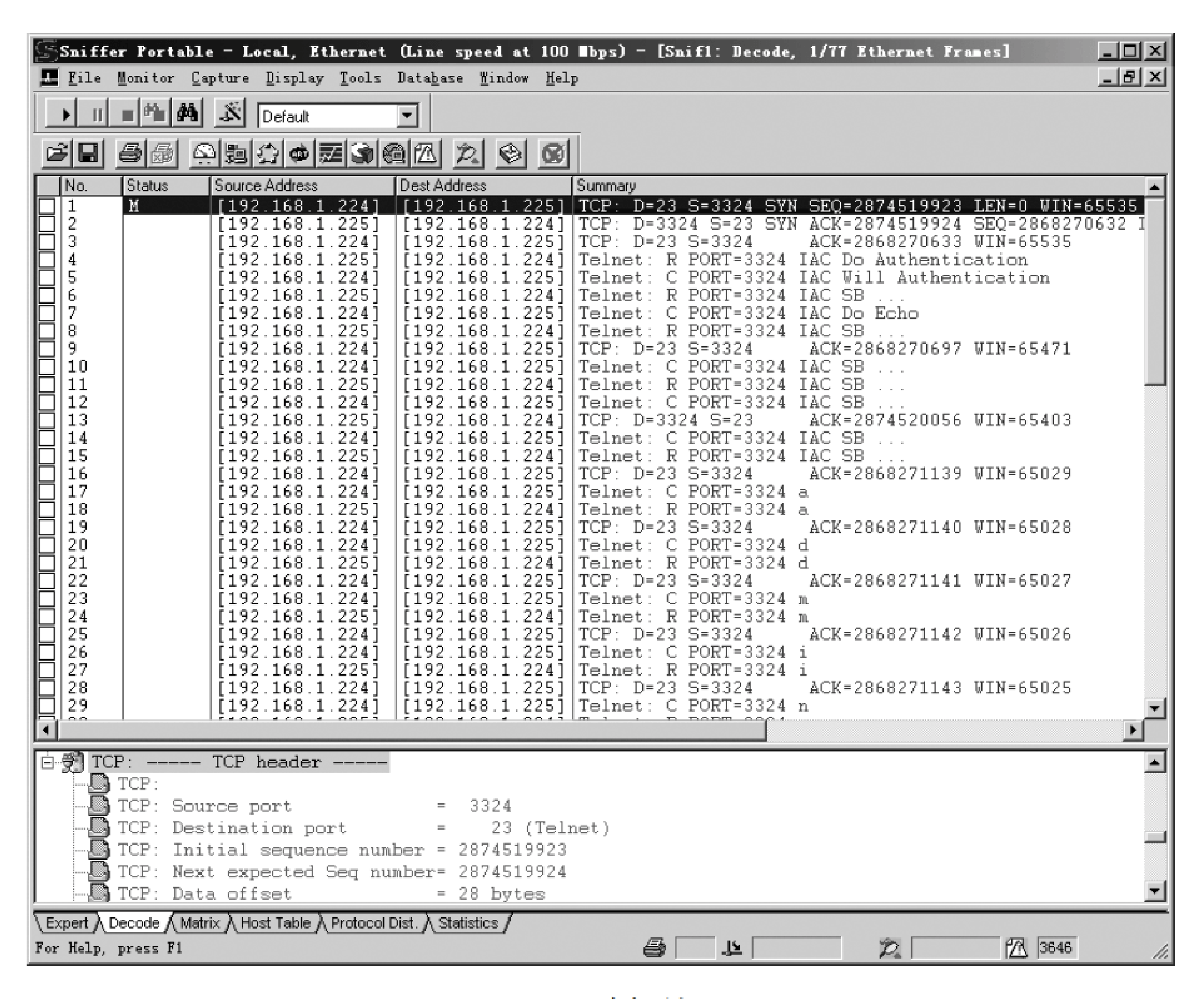


图 3.52　嗅探结果

客户端 Telnet 到服务器端时，一次只传送一个字节的数据；由于协议的头长度是一定的，所以 Telnet 的数据包大小＝DLC(14 字节)＋IP(20 字节)＋TCP(20 字节)＋数据(1 字节)，共 55 个字节，因此，可以将图 3.49 的 Packet Size 设为 55，以便捕获到用户名和密码；如图 3.53 所示，设定为仅捕获客户端到服务器端的数据包，过滤其他类型的干扰数据包。

再次重复捕获过程，即可显示用户名和明文密码，如图 3.54 所示，用户名为“administrator”，密码为“123456”。

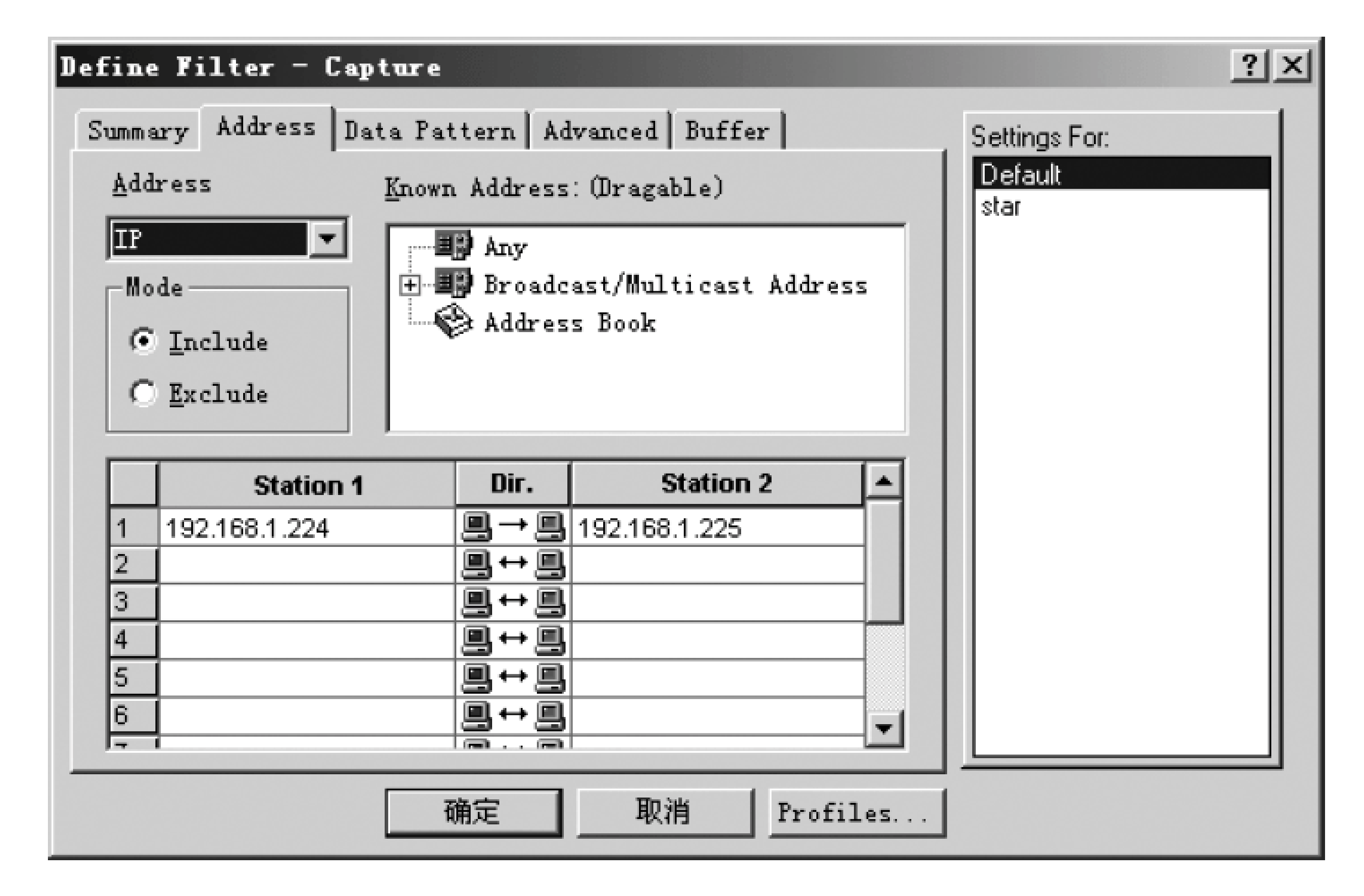


图 3.53 设定为仅捕获客户端到服务器端的数据包

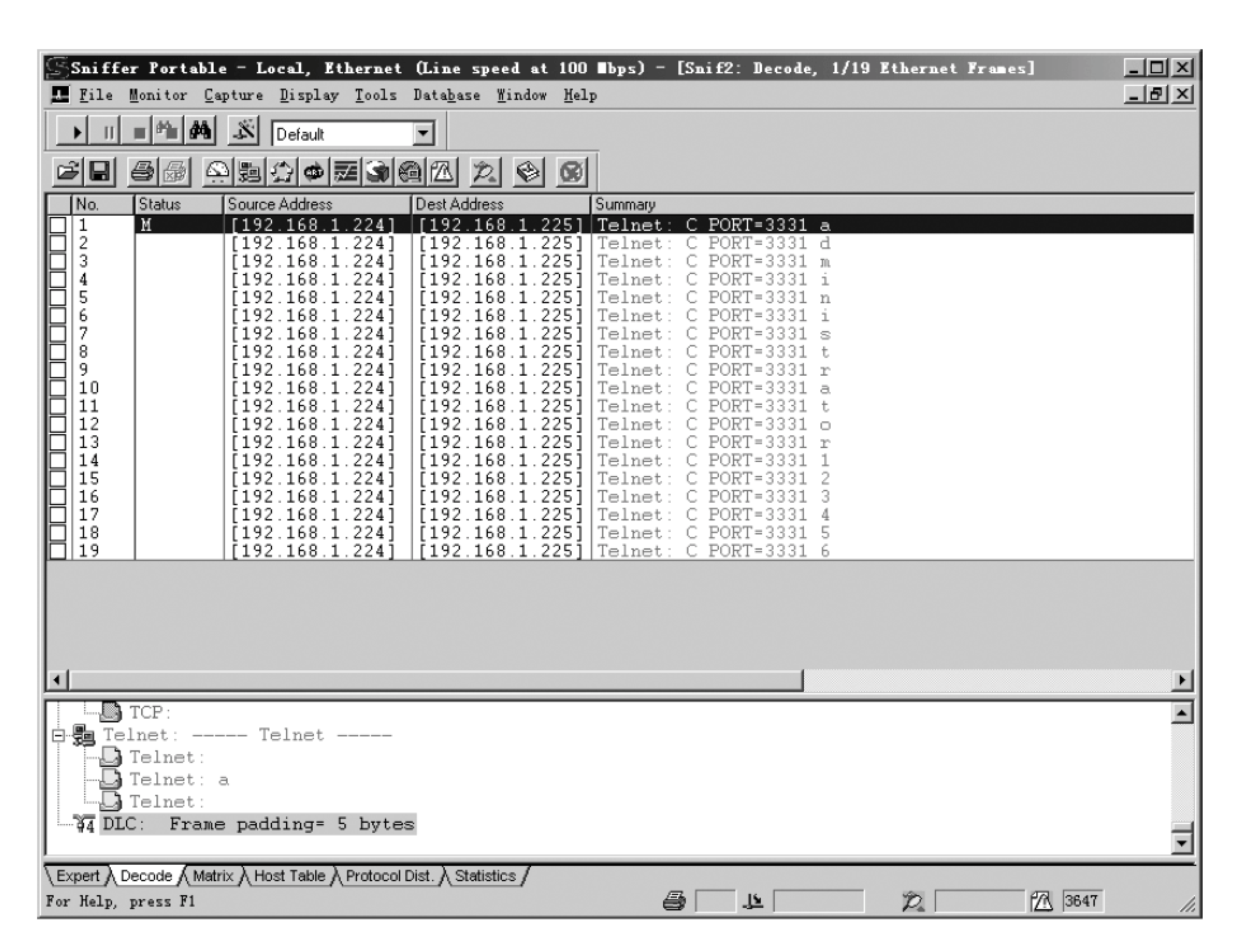


图 3.54 用户名和明文密码

思考题

(1) 如何捕获 HTTP 协议下的用户名和密码?

(2) 分析 TCP 协议的头结构,以及两台主机之间建立连接的过程。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

3.3.4 多协议综合实验

实验器材

- Sniffer Pro 软件系统 1 套。
- PC(Windows XP/Windows 7)1 台。

预习要求

- 做好实验预习,复习网络协议有关内容。
- 复习 Sniffer 软件的操作方法。
- 熟悉实验过程和基本操作流程。
- 做好预习报告。

实验任务

通过本实验,理解和掌握 Sniffer 的综合应用;明确 FTP、TCP、ICMP 等多种协议的数据传输问题;理解主要协议的结构。

实验环境

本实验采用一个已经连接并配置好的局域网环境。所有 PC 上安装的都是 Windows 操作系统。本次实验需在小组合作的基础之上完成。每个小组由两位成员组成,相互之间通信,通过 Sniffer 工具截取通信数据包,分析数据包完成实验内容。

实验步骤

(1) 填写小组情况表,通过 ipconfig 命令获取本机 IP 地址,并填写表 3.4。

表 3.4 小组情况表

小组成员姓名	机器 IP 地址	本机用户名
A	192.168.1.136	User36
B	192.168.1.137	User37

(2) 开启 Sniffer Pro 软件,自定义过滤器设置,并进入捕获状态。

(3) 从本机 ping 小组另一位成员的计算机,使用 Sniffer 截取 ping 过程中的通信数据。

(4) 分析第(3)步操作从本机发送到目标机器的 IP 数据,并填写表 3.5。

表 3.5 IP 数据报表

IP 协议版本号(IPv4/IPv6)	
服务类型(使用中文明确说明服务类型,比如“要求最大吞吐量”)/b	
IP 报文头长度/bytes	
数据报总长度/bytes	
标识	
数据报是否要求分段	

分段偏移量	
在发送过程中经过几个路由器	
上层协议名称(ICMP)	
报文头校验和	
源地址(IP)	
目标地址(IP)	

(5) 分析第(3)步操作从目标机器返回到本机的数据帧中的 IP 数据报,并填写表 3.5。

(6) 从本机通过 telnet 命令远程登录小组另一位成员的计算机,然后使用 dir 文件查看对方 C 盘根目录下的文件系统结构,最后使用 exit 命令退出。使用 Sniffer 截取操作中的通信数据。

(7) 分析第(6)步操作从本机发送到目标机器的数据帧中的 TCP 数据,填写表 3.6。

表 3.6 通信报表

数据发送端口号	
通信目标端口号	
TCP 报文序号	
TCP 报文确认号	
下一个 TCP 报文序号	
标志位含义(如“确认序号有效”)	
窗口大小	
校验和	
源 IP 地址	
目标 IP 地址	

(8) 分析第(6)步操作从目标机器返回到本机的数据帧中的 TCP 数据,并填写表 3.6。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

第 4 章　远程控制实验

4.1　远程控制原理

所谓远程控制，是指管理人员在异地通过计算机网络联通被控制的计算机，将被控计算机的桌面环境显示到自己的计算机上，通过本地计算机对远端计算机进行配置、软件安装、文件编辑等工作。这里的远程指的是通过网络控制远端计算机。当操作者使用主控计算机控制被控端计算机时，可以启动被控端计算机的应用程序，使用被控端的文件资料，甚至可以利用被控端计算机的外部设备和通信设备来进行工作。

远程控制必须通过网络才能进行。位于本地的计算机是操纵指令的发出端，称为主控端或客户端；非本地的被控计算机叫做被控端或服务器端。

4.1.1　远程控制技术

随着网络的快速发展，为满足计算机管理及技术支持需要，远程操作及控制技术越来越引起人们的关注。远程控制支持多种网络方式：LAN、WAN、拨号方式及互联网方式。此外，远程控制还支持通过串口、并口、红外端口来对目标主机进行控制。传统的远程控制技术一般使用 NETBEUI、NETBIOS、IPX/SPX、TCP/IP 等协议来实现，此外，还支持 Java 技术，实现不同操作系统下的远程控制。远程控制的工作原理如图 4.1 所示。

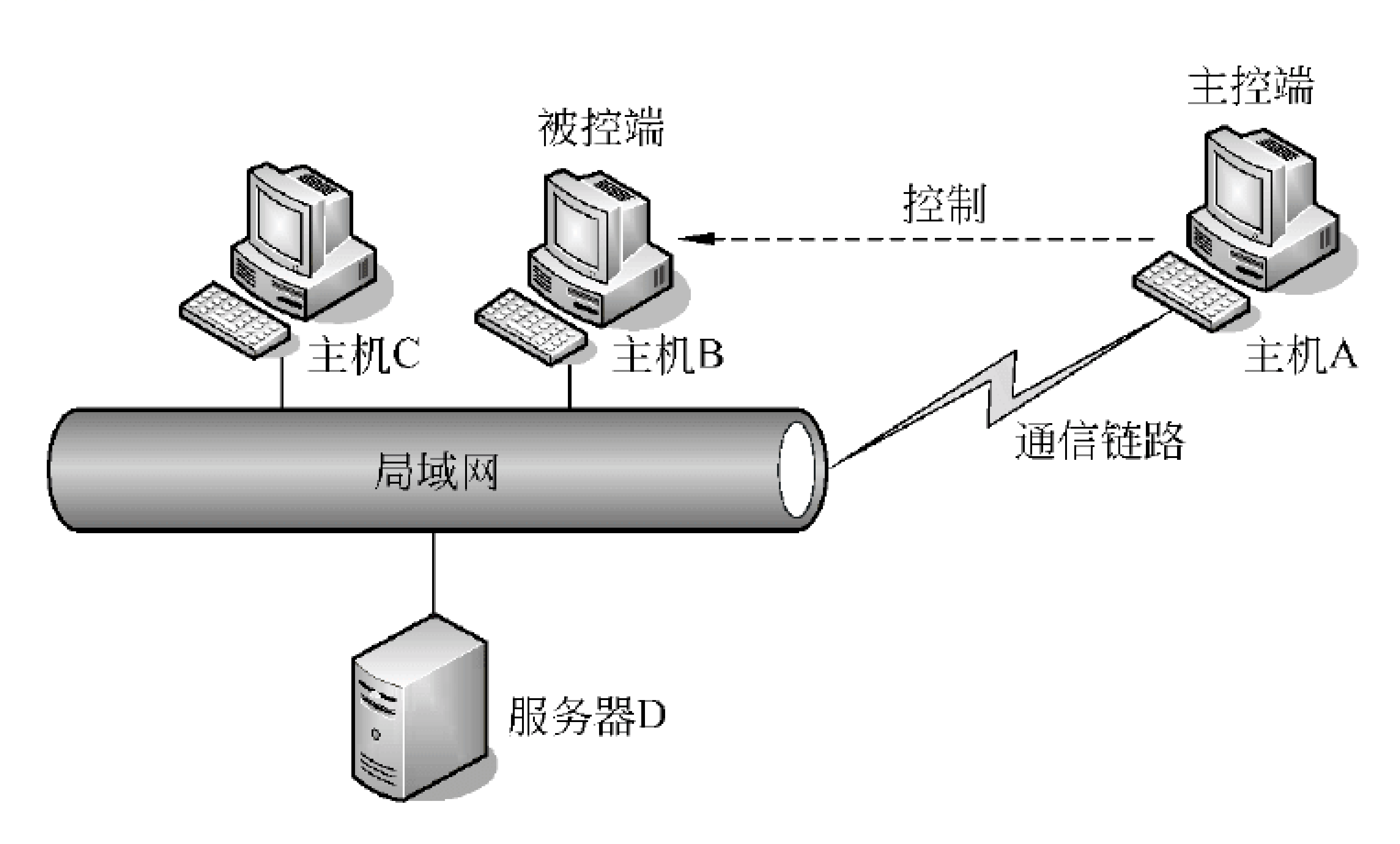


图 4.1　远程控制的工作原理

远程控制由两部分组成：客户端程序(Client)和服务器端程序(Server)。在进行远程控制前，需要事先将客户端程序安装到主控端计算机上，服务器端程序安装到被控端计算机上。对于 Windows XP 或 Windows Server 2003 操作系统而言，可以利用随机自带的系统程序实现远程控制。

远程控制的过程是先在主控端计算机上执行客户端程序，向被控端计算机中的服务器端程序发出信号，建立一个特殊的远程服务；通过这个远程服务，使用远程控制功能发

送远程控制命令，控制被控端计算机运行。

4.1.2 远程控制方式

远程控制的实现方式通常有两种：点对点方式和点对多点方式。

如图 4.2 所示，Windows XP 或 Windows Server 2003 操作系统的主机通常采用点对点工作方式。点对点控制指的是一个远程客户端的程序在同一时间内只能连接并控制唯一一台远程计算机。点对点控制程序的工作模式是客户端控制服务器端，这也是远程访问控制中运用最普遍的情况。点对点的访问控制主要应用于对远程主机进行具体控制和监控的需求。

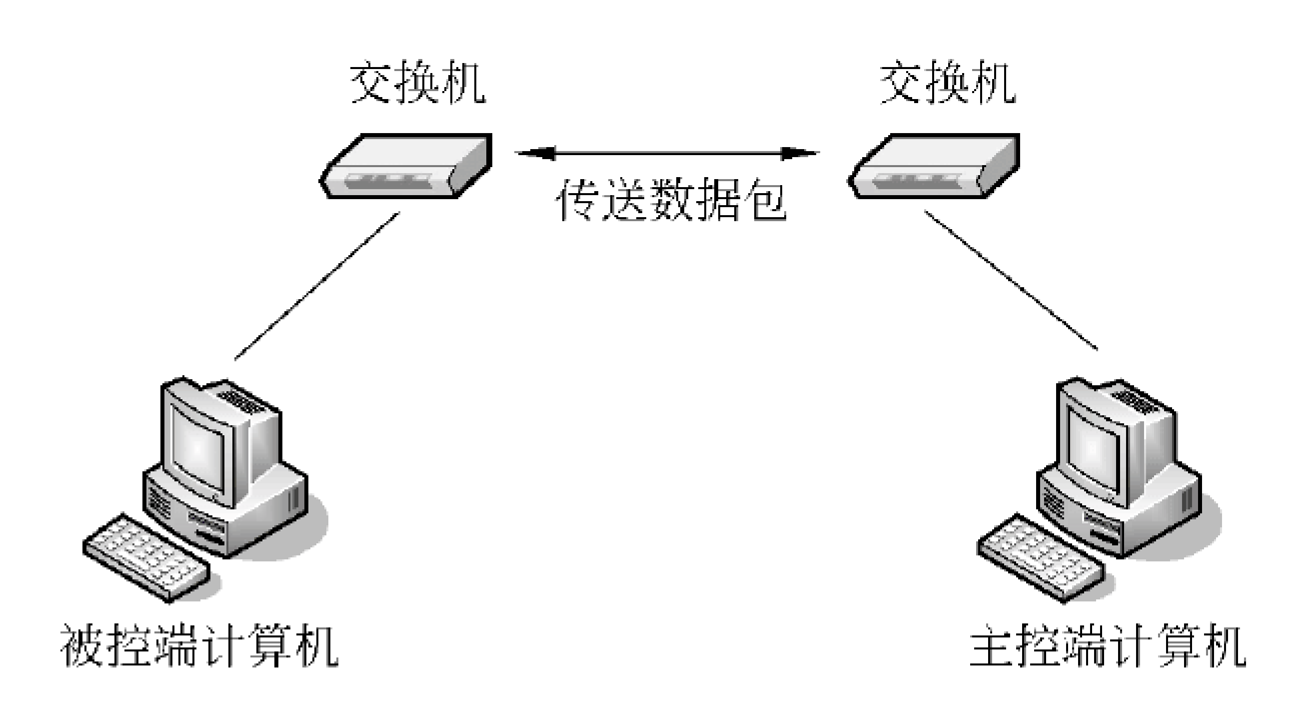


图 4.2 远程控制的点对点方式

一些专业软件，如远程控制软件 pcAnywhere，可以借助局域网优势用一台计算机控制多台计算机，实现对远程主机的多点控制，如图 4.3 所示。点对多点的访问控制可以在同一时间内对一台或多台远程计算机进行控制，但点对多点的访问控制机制并不会比点对点的访问控制功能更加具体和强大。点对多点的访问控制流程和点对点相反，首先由每个客户端程序向服务器端程序发出连接请求，建立连接之后，服务器端就可以对多台远程计算机的客户端程序发出指令并由客户端程序执行指令。点对多点的访问控制主要应用于控制大范围计算机领域，诸如定时、收费、监督等需求。

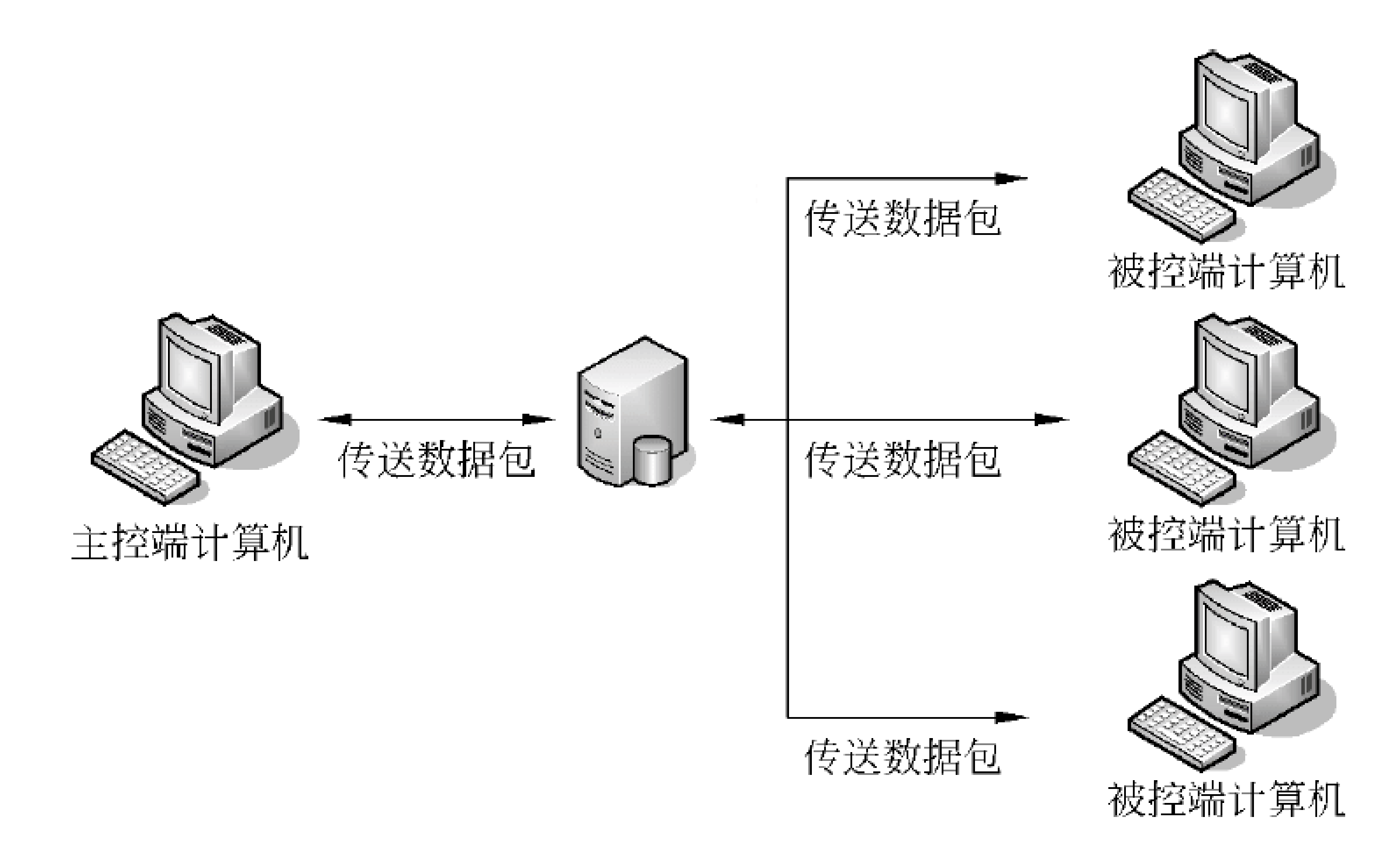


图 4.3 远程控制的点对多点方式

远程控制在计算机网络管理与维护中应用相当普遍，网络管理员可以接入局域网中的任意一台计算机，通过远程控制方式对网内服务器等设备进行管理和维护，实现在服务

器上进行软件安装、系统升级、数据备份以及日志查看等功能。

4.1.3 远程控制软件

随着数字信息处理需求越来越广泛，远程控制越来越多地被应用到人类生活和办公当中，这其中包括三款国内外著名的远程控制软件。

4.1.3.1 软件简介

1. DLinkPC（中国）

DLinkPC 是一款目前国内集远程控制、远程开关机、监控和 VPN 为一体的远程服务平台。只要申请用户名，在被控制的计算机里运行被控端，登录后设置好远程访问的密码，就可用主控端，通过相同的用户名和远程访问密码进行远程桌面控制、下载/上传文件。

2. TeamViewer（德国）

TeamViewer 可以在任何防火墙和 NAT 代理后台进行远程控制、桌面共享和文件传输。为了连接到另一台计算机，需要在两台计算机上同时运行 TeamViewer。软件第一次启动时，在两台计算机上自动生成伙伴 ID，只需要输入伙伴 ID，TeamViewer 就会立即建立起连接。这款软件是至今唯一的一款能穿透内网的远程控制软件，可以穿透各种防火墙，任何一方都不需要拥有固定 IP 地址，双方可以相互控制。

3. pcAnywhere（美国）

pcAnywhere 是一款独特的集成解决方案，它结合了远程控制、远程管理、高级文件传输功能和强健的安全性，可以提高技术支持效率并减少呼叫次数。使用 pcAnywhere 可实现对 Linux 和 Windows 系统的远程管理，从而避免使用命令行工具。使用被控端会议功能，可以建立起一个 pcAnywhere 被控端的多个并发远程连接。

4.1.3.2 性能比较

1. 安全性对比

（1）DLinkPC：登录被控端软件后，需要设置一系列安全选项（如远程访问权限、远程访问功能、远程访问密码等），如图 4.4 所示。

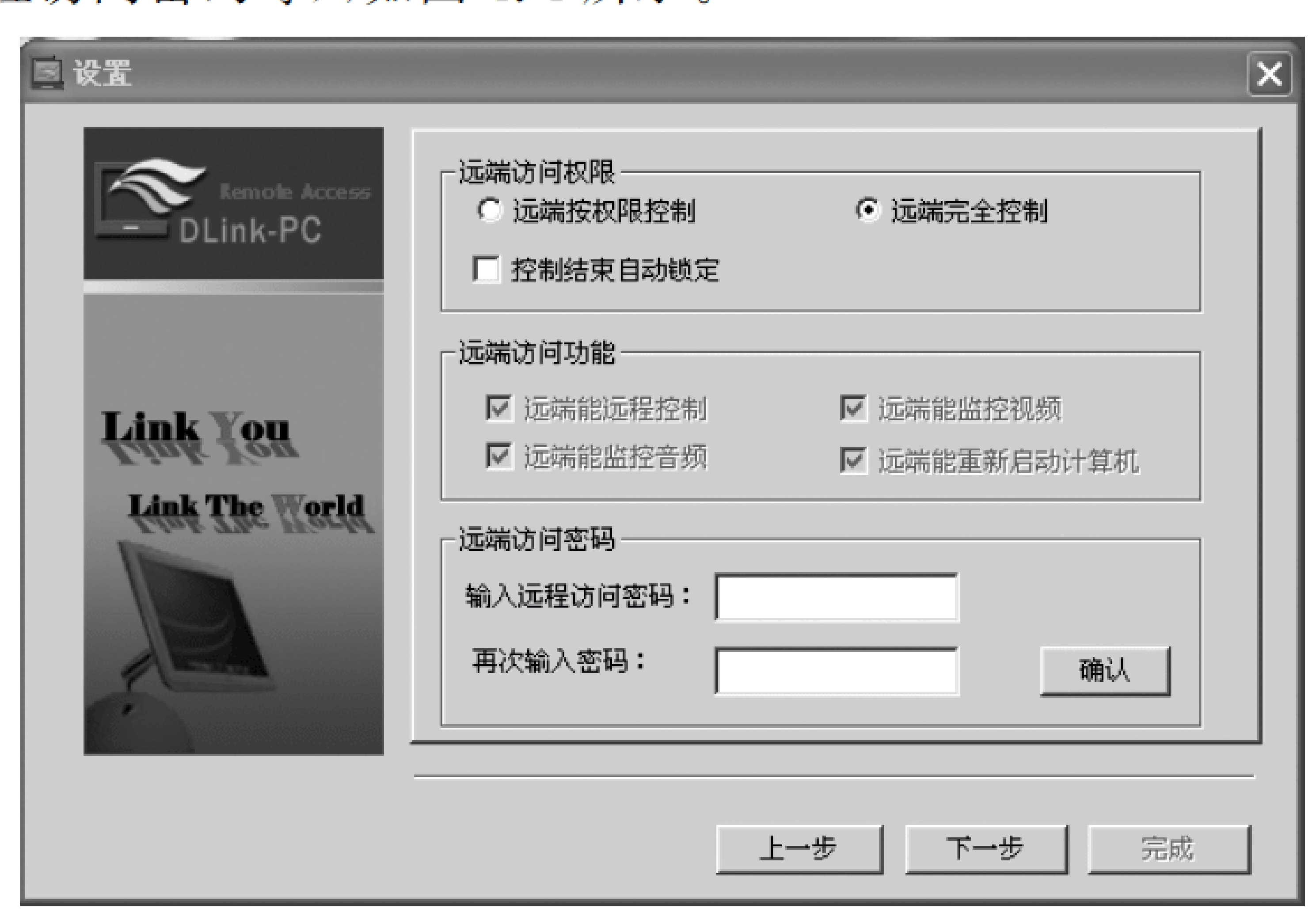


图 4.4 DLinkPC 访问设置

(2) TeamViewer：在软件选项中设置固定密码，既增加安全性，又确保密码不会变化。根据安全级别设置访问权限，限制控制方的操作权限，如图 4.5 所示。

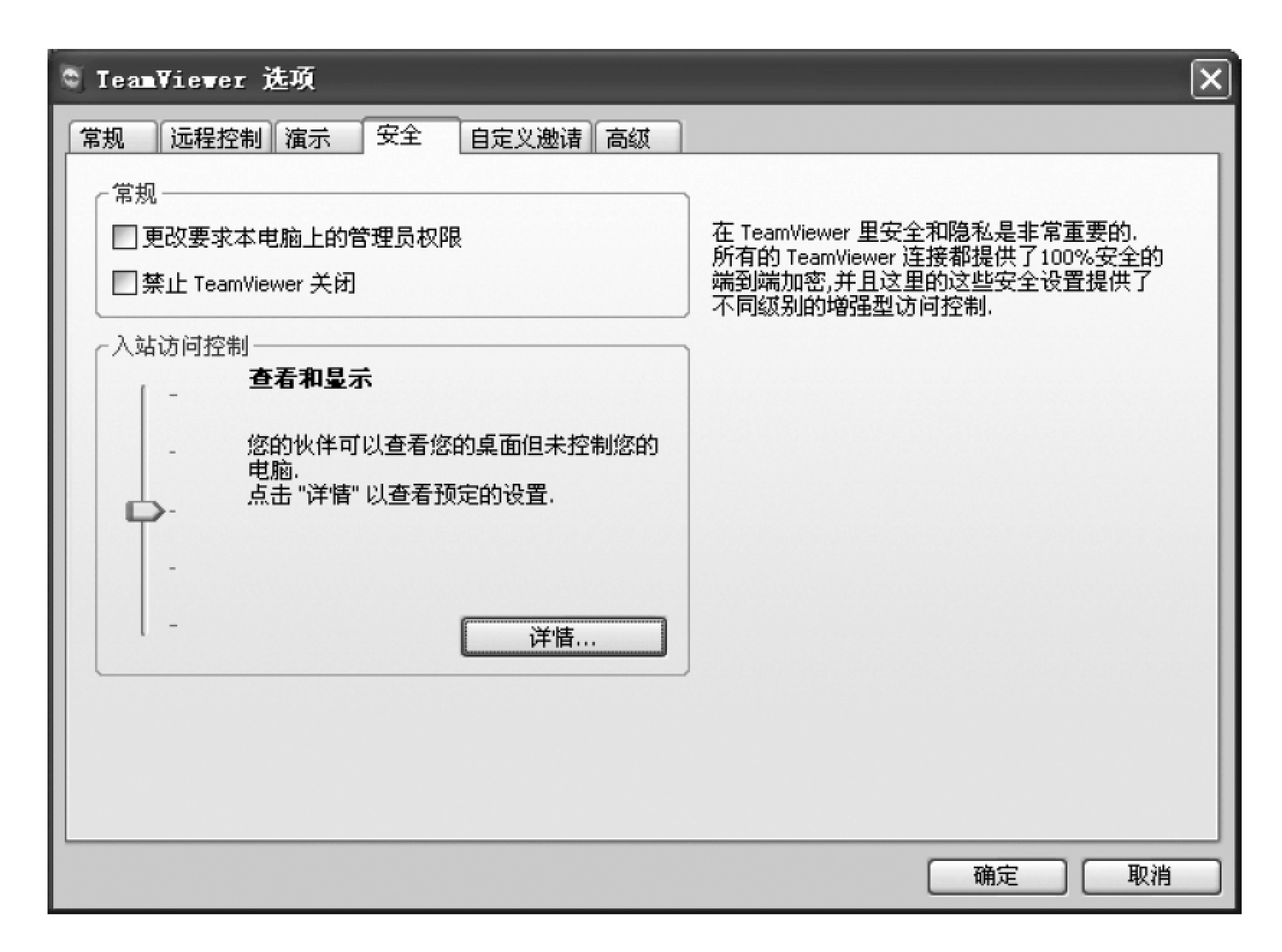


图 4.5 TeamViewer 访问设置

(3) pcAnywhere：允许被控方主动设置用户名、密码；在主控端，可以设置连接时的加密级别，为主控端设定密码，提高远程访问过程的安全性。

2. 服务器响应速度对比

服务器响应速度如表 4.1 所示。

表 4.1 服务器响应速度

软件名称	服务器响应时间	软件名称	服务器响应时间
DLinkPC	3～8 秒	pcAnywhere	不需要服务器
TeamViewer	5～8 秒		

3. 操作方式对比

(1) DLinkPC：软件分为主控端、被控端以及临时客户端三个部分。在网站上注册好账号，登录两端程序，就可以在列表中看到被控端上线，并进行控制。如果没有申请账号可以让控制端生成临时账号，在临时客户端登录，也能进行控制。

(2) TeamViewer：软件把两端的功能进行整合，软件安装后的主机既可作为主控端，也可作为被控端。只要得到对方的 ID 以及密码，就可以进行远程协助或者控制。

(3) pcAnywhere：程序必须同时安装在主控和被控计算机中。在主控端计算机中，可通过“联机向导”命令，利用随后打开的向导对话框去创建主控端，与主控端的创建方式不同，在创建被控端向导中可设定连接的用户名及密码。

pcAnywhere 是赛门铁克公司的著名产品，该软件适用于所有版本的 Windows 操作系统。该软件的使用与管理方式比较灵活，用户可以按照自己的需要单独安装主控端或被控端的软件，根据需要在被控端上创建各种连接下的远程控制方案，并能根据不同的用户分配不同等级的权限。在安全性能方面，pcAnywhere 提供了多种验证方式和加密方式，用户可以直接使用网络系统的用户资料库验证远程连接，也可以创建独立的远程控制账户，根据需要选择加密数据方式，保证传输过程中数据不被窃取。

3 种软件性能的整体对比如表 4.2 所示。

表 4.2　软件主要功能

主 要 功 能	DLinkPC	TeamViewer	pcAnywhere
远程开机	√	×	√
远程控制桌面	√	√	√
远程复制、粘贴文字	√	√	√
允许多重连接	√	×	√
Windows 账户验证	×	×	×
文件管理(文件上传、下载)	√	√	√
文件搜索功能	×	×	×
文件断点续传	√	√	×
语音视频	√	√	×
桌面、视频、语音录像	√	√	×
远程旋转视频监控	√	√	×
VPN	√	√	×
自动升级	×	×	×
查看登录记录	√	√	√
隐性功能(隐藏软件)	×	×	×
强制中转(穿透代理上网)	×	×	×

4.2　pcAnywhere 远程控制实例

4.2.1　软件的安装与使用

实验器材

- pcAnywhere 软件系统 1 套。
- PC(Windows XP/Windows 7)1 台。

预习要求

- 做好实验预习,复习远程控制技术的有关内容。
- 复习 pcAnywhere 软件的操作方法。
- 熟悉实验过程和基本操作流程。
- 做好预习报告。

实验任务

通过本实验,学会在 Windows 环境下安装 pcAnywhere。

实验环境

本实验采用一个已经连接并配置好的局域网环境。PC 上安装 Windows 操作系统。

预备知识

- 远程控制原理及基本协议。
- 远程控制技术概念及原理。

实验步骤

pcAnywhere 分为 Full、Host 以及 Remote 等版本,可以根据实际需要选择不同的版本来安装。本实验所使用的 pcAnywhere 的版本是 V12.5。

(1) 打开 pcAnywhere V12.5 的主安装文件 Symantec pcAnywhere v12.5.exe,进入安装界面,如图 4.6 所示。



图 4.6 pcAnywhere 安装界面

(2) 在许可协议中选择"我接受许可协议中的条款",并单击"下一步"按钮。

(3) 在客户信息中填写"用户名"和"组织",如图 4.7 所示。

(4) 在"安装位置设置"中选择 pcAnywhere 的安装磁盘位置,默认路径即可。

(5) 在"自定义安装"的自定义设置中,作为主机管理员,可以选择典型安装,即主机管理员和主机管理员代理;但作为被控端,需要同时选择这两项,如图 4.8 所示。



图 4.7　填写用户名和机构名称注册



图 4.8　安装代理管理工具

(6) 选中 Symantec pcAnywhere，意思是在桌面上放置 pcAnywhere 的快捷方式，单击“下一步”按钮。

(7) 安装 pcAnywhere 的主要程序，完成 pcAnywhere 的安装。

(8) 打开桌面上的图标 Symantec pcAnywhere，如图 4.9 所示。

(9) 单击“转到高级视图”选项，界面左侧会有各种选择项，如图 4.10 所示。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。



图 4.9 运行界面

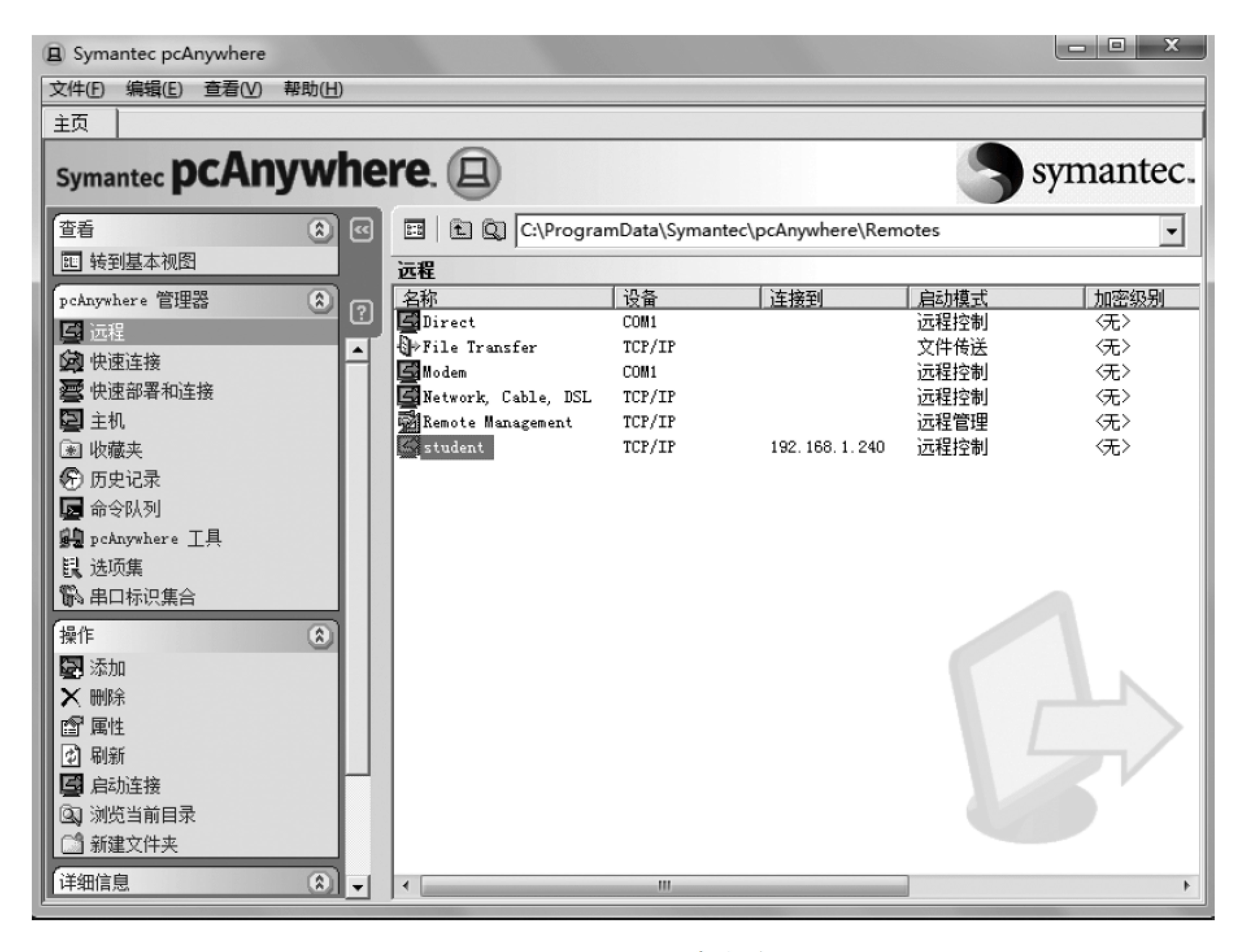


图 4.10 pcAnywhere 高级视图

4.2.2 配置被控端(hosts)

实验器材

- pcAnywhere 软件系统 1 套。
- PC(Windows XP/Windows 7)1 台。

预习要求

- 做好实验预习，复习远程控制技术的有关内容。
- 复习 pcAnywhere 软件的操作方法。
- 熟悉实验过程和基本操作流程。
- 做好预习报告。

实验任务

通过本实验，学会在 Windows 环境下安装 pcAnywhere 被控端。

实验环境

本实验采用一个已经连接并配置好的局域网环境。PC 上安装 Windows 操作系统。

预备知识

- 远程控制原理及基本协议。
- 远程控制技术概念及原理。

实验步骤

(1) 选择界面中的主机后，单击添加功能，进入被控端的连接向导，选择"我想使用电缆调制解调器/DSL/LAN/拨号互联网 ISP"单选项，单击"下一步"按钮，如图 4.11 所示。

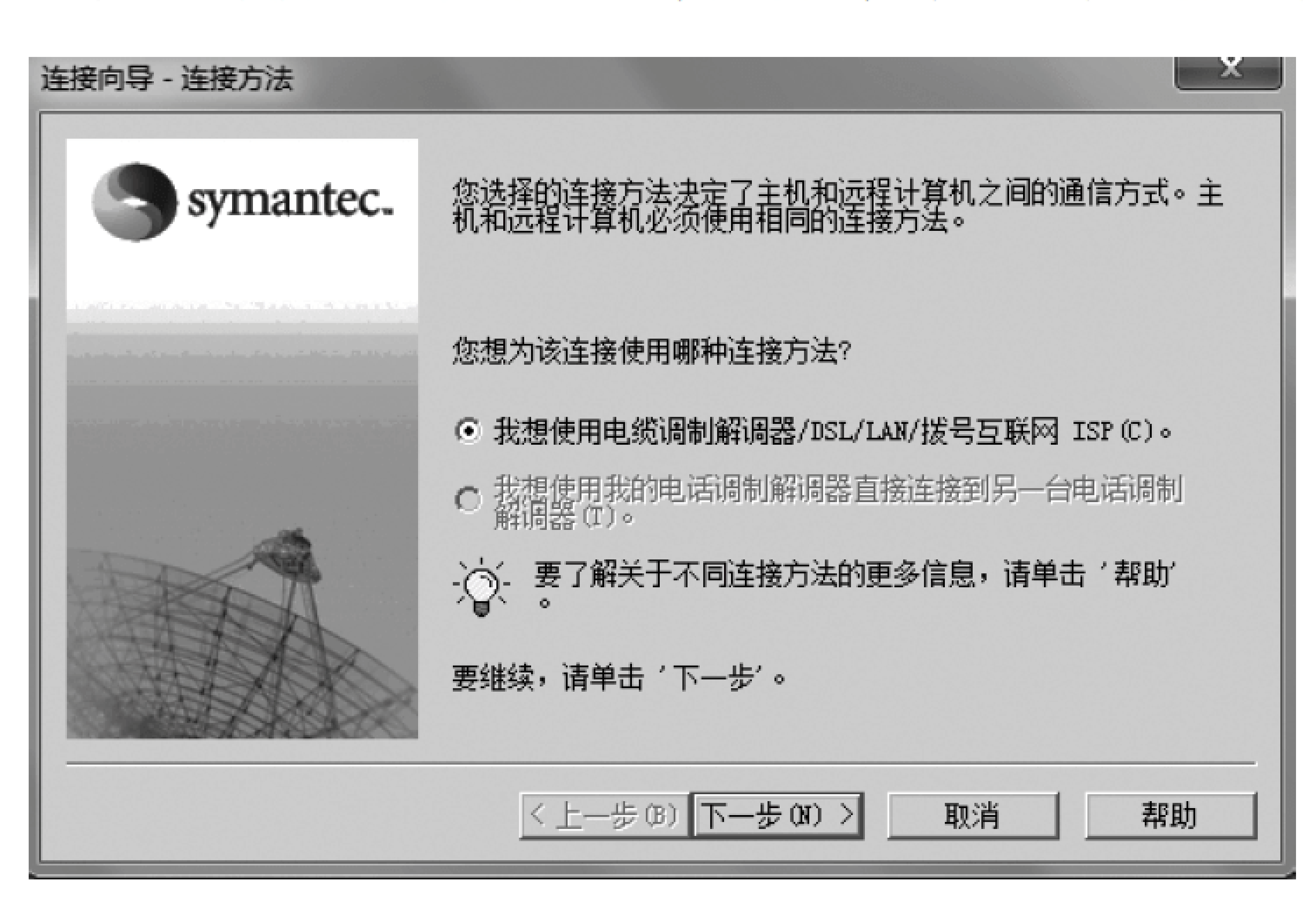


图 4.11　添加被控端选项

(2) 选择连接模式，选择"等待有人呼叫我"。

(3) 在验证类型中选择第一个选项则使用 Windows 现有账户，选择第二个选项则是创建 pcAnywhere 新的用户和密码，如图 4.12 所示。

(4) 在此过程中，需要选择 Windows 用户，如图 4.13 所示。

(5) 单击"下一步"按钮，默认创建完成。允许用户再次确认连接选择，并选择是否连接完成后等待来自远程计算机的连接。在创建完后程序会提示对新主机进行命名，例如，命名为"student"。右击需要配置的连接项目，选择"属性"窗口，更改属性，如图 4.14 所示。

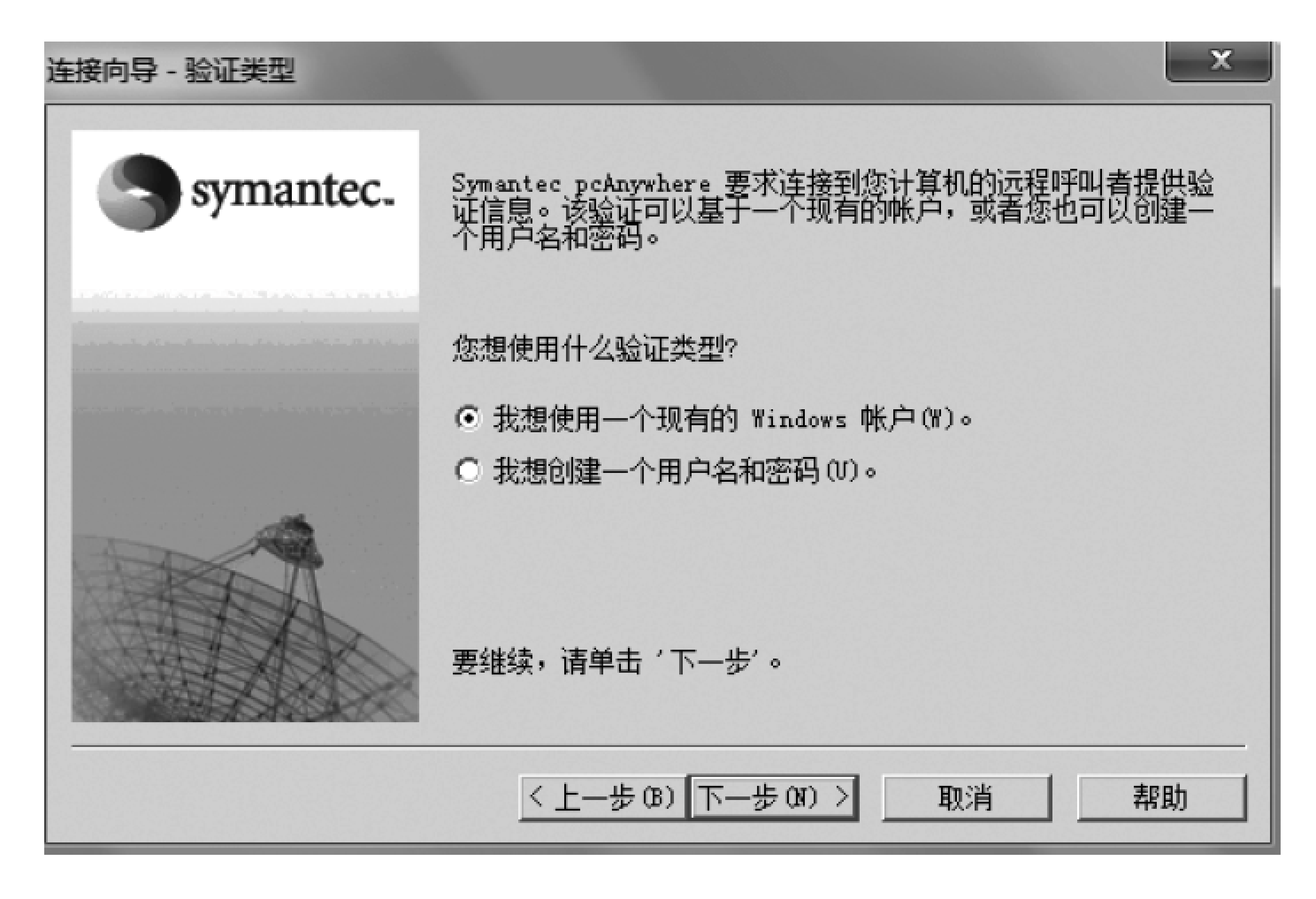


图 4.12　建立账户

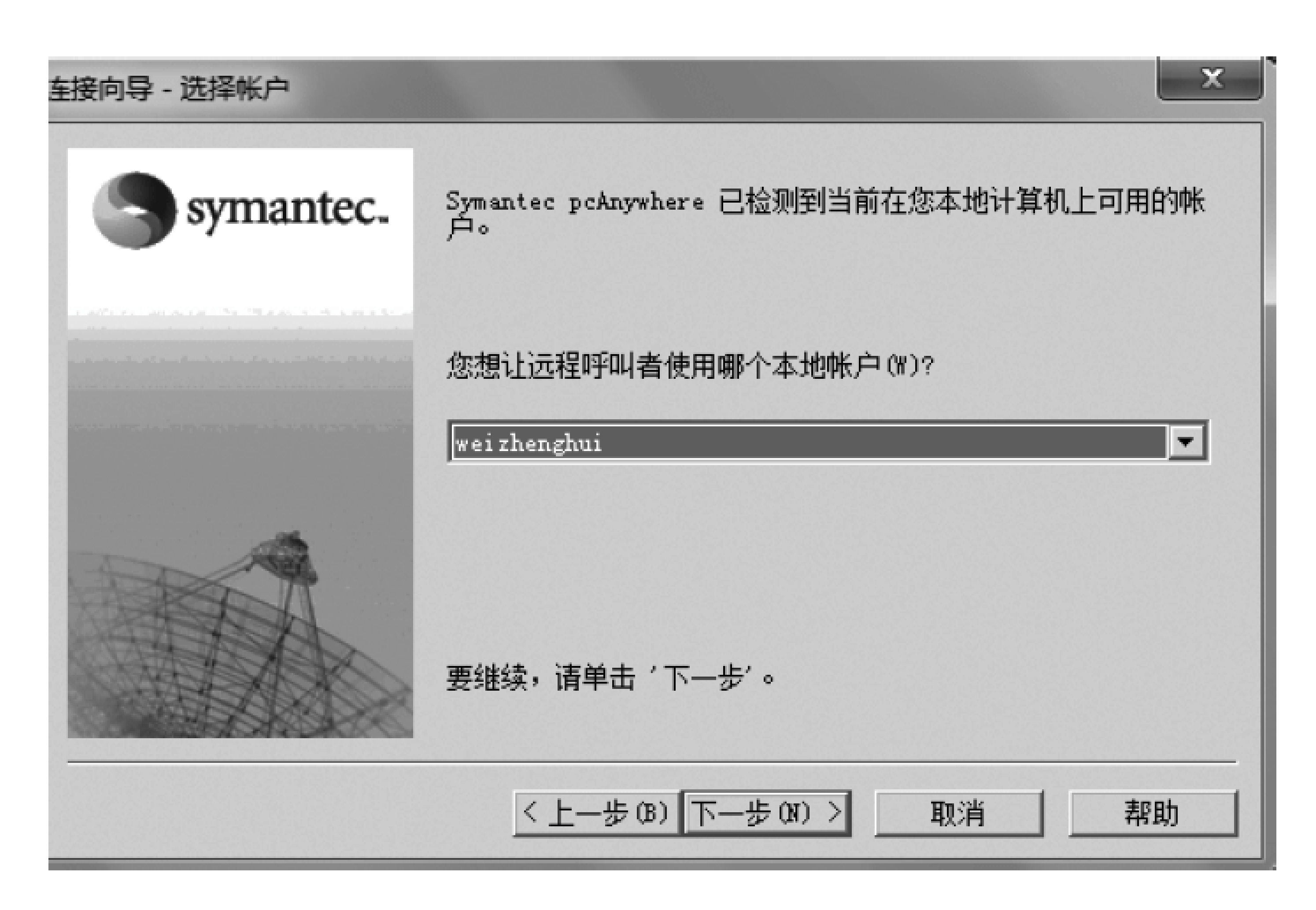


图 4.13　选择账户



图 4.14　属性配置窗口

① 连接信息：指的是建立连接时所使用的协议。一般默认 TCP/IP，可以根据实际需要选择合适的协议，本实验以常见的 TCP/IP 协议为例，如图 4.15 所示。

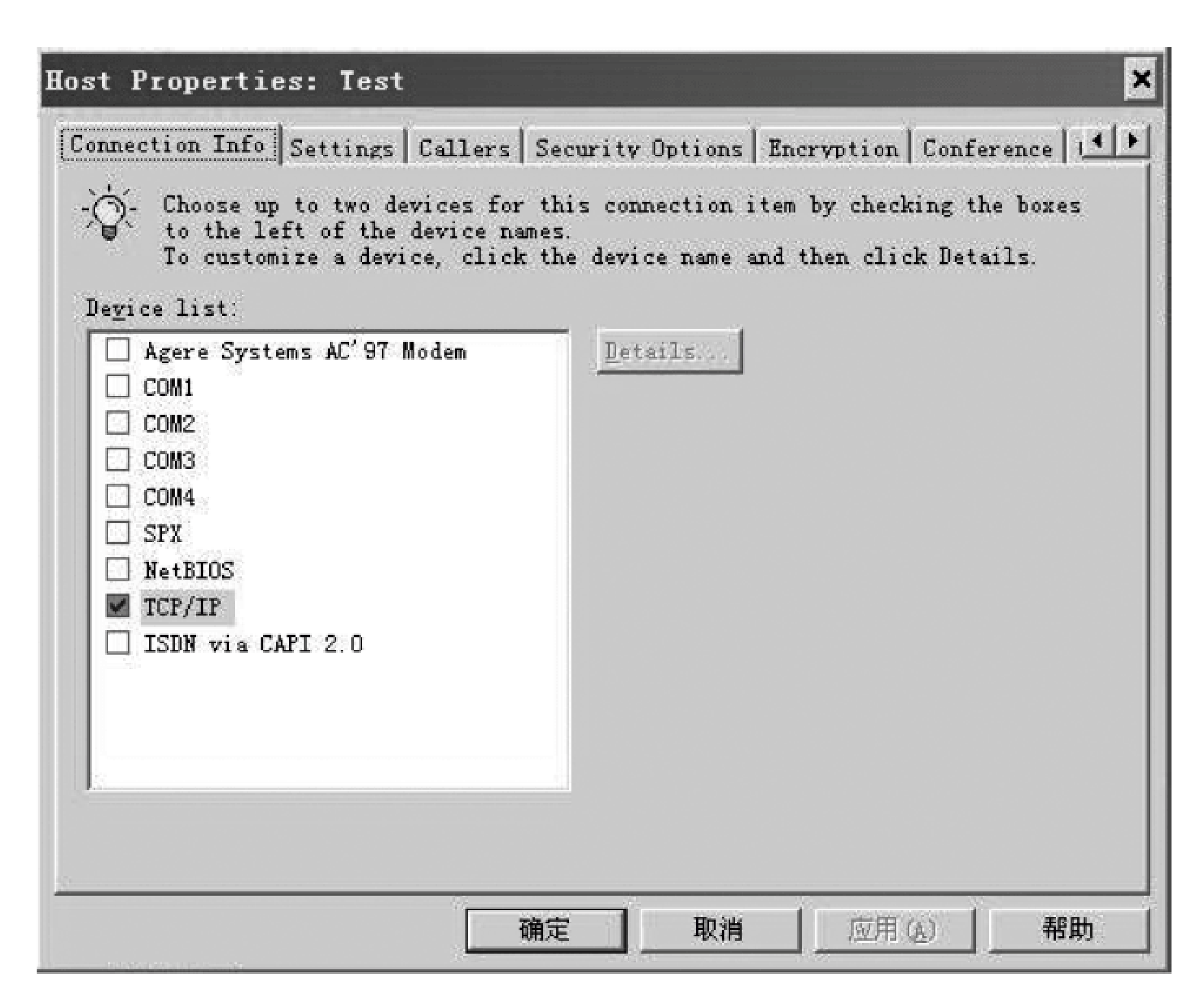


图 4.15　确定连接协议

② 设置：远程控制中，被控制端只有建立安全机制，才能有效地保护系统不被恶意控制所破坏。

- “随 Window 一起启动”和“运行最小化”指的是被控制端配置好以后，决定是否下次启动计算机时就直接启动 pcAnywhere，并且让 pcAnywhere 最小化，这是一个可以复选的选项。
- “会话非正常结束后”指的是在连接会话不正常的情况下（比如连接突然中断），是否就放弃连接，还是等待下一次连接。
- “且由以下确保安全”指的是为了保护本机安全，可以选择锁定用户，不允许其他的控制端登录、重新启动计算机等。

③ 呼叫者：指的是可以创建连接到本机的用户账号及密码。在这里设置允许哪些用户进行远程控制以及分配控制权限，单击“新建”按钮，弹出设置新用户的对话框，设置好一个新的用户名和登录密码，以及相应的权限，单击“确定”按钮保存，如图 4.16 所示。“验证类型”选择 pcAnywhere。

图中的用户“teacher” 就是在创建连接向导时创建的用户，如果有需要可以单击红色标签按钮进行新用户的添加。同样可以双击“用户设置”进行配置，如修改管理密码（如图 4.17 所示）、设置用户特权等。

④ 安全：指可以设置本机的安全策略。

- 连接选项：连接成功以后，可以选择是否清除本机屏幕上的显示；是否相隔确定时间确认一次连接是否仍然有效（提示确认连接）。
- 登录选项：可以限制对本机进行登录的次数与时间，默认值是每个人只允许登录三次，每一次登录所用的时间是三分钟。

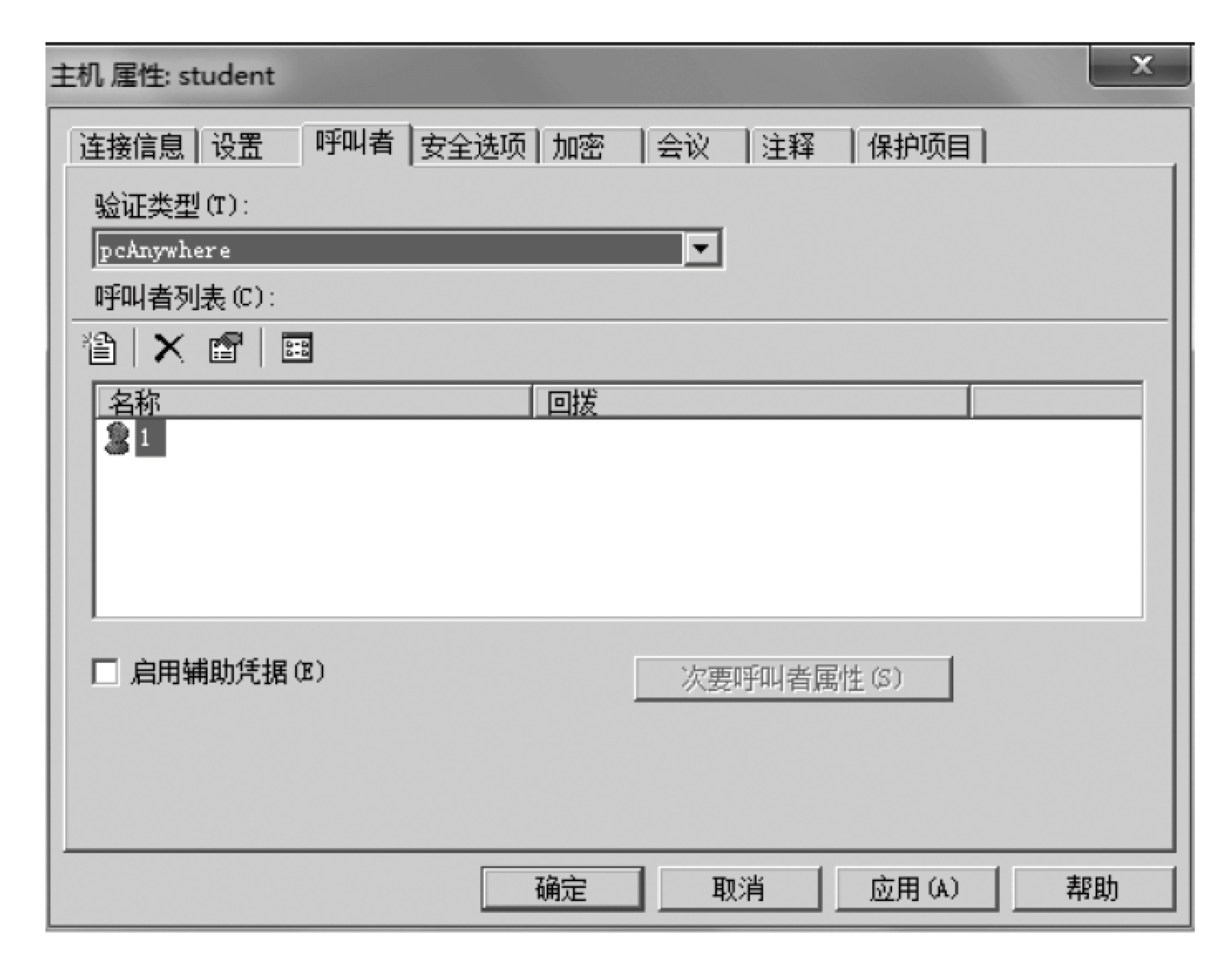


图 4.16　呼叫者设置

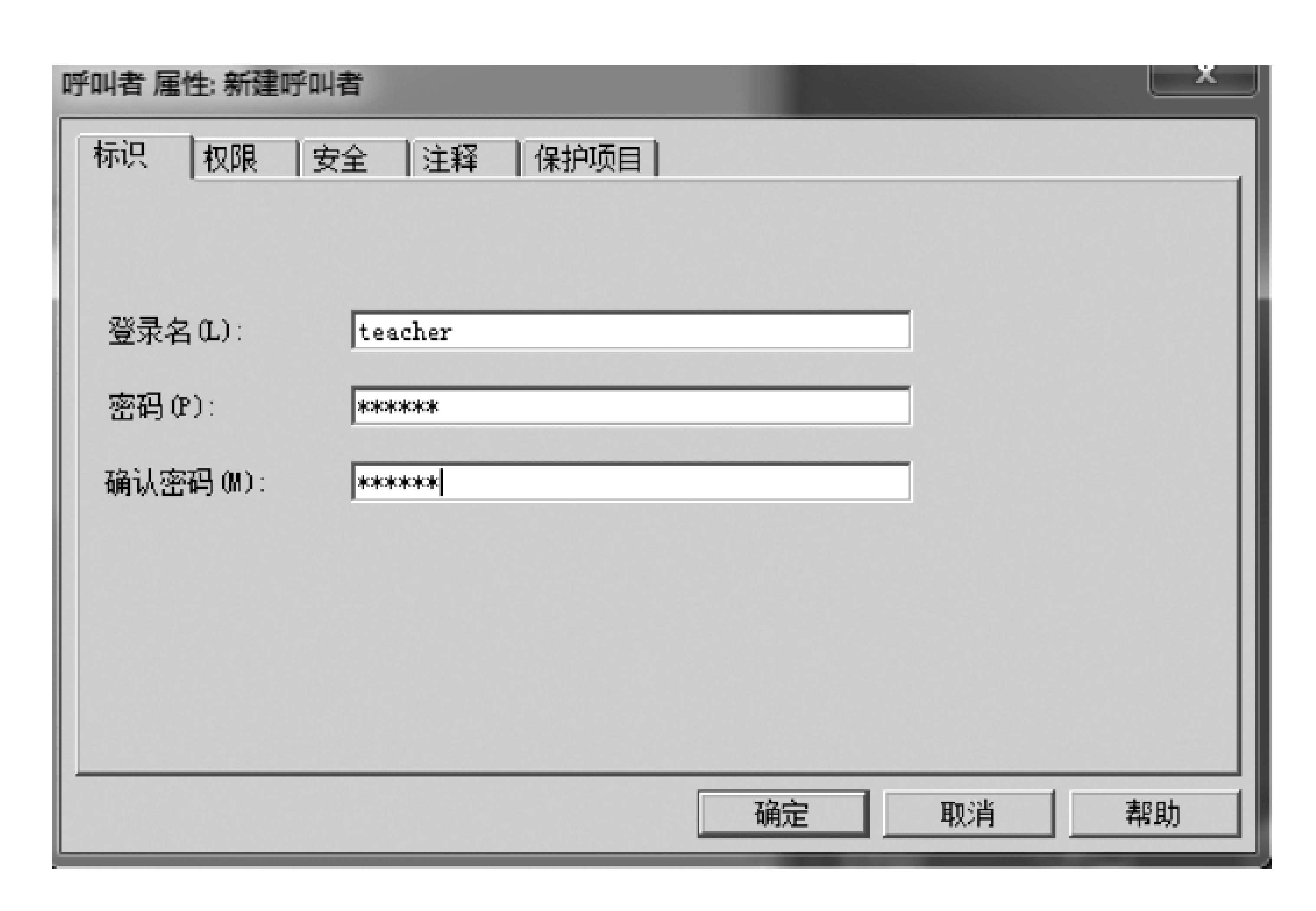


图 4.17　用户特权设置

⑤ 保护项目：允许用户输入密码来保护当前设置的被控端选项，保护后任何人试图查看或更改该被控端的选项时，都将需要输入密码来确认。以上属性都配置好以后，单击“确定”按钮完成被控端设置。

右击被控端图标，选择“运用主机”，被控端将启动并在系统任务栏上显示一个计算机形状的图标，开始等待远程控制的主控端进行连接。当用户远程连接时，图标改变颜色。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

4.2.3 配置主控端(Remotes)

实验器材

- pcAnywhere 软件系统 1 套。
- PC(Windows XP/Windows 7)1 台。

预习要求

- 做好实验预习,复习远程控制技术的有关内容。
- 复习 pcAnywhere 软件的操作方法。
- 熟悉实验过程和基本操作流程。
- 做好预习报告。

实验任务

通过本实验,学会在 Windows 环境下安装 pcAnywhere 的主控端。

实验环境

本实验采用一个已经连接并配置好的局域网环境。PC 上安装 Windows 操作系统。

预备知识

- 远程控制原理及基本协议。
- 远程控制技术概念及原理。

实验步骤

设置好被控端后,另一项十分重要的工作就是配置主控端计算机。

(1) 在管理窗口中,单击“远程”,通过这个页面可以完成主控端连接项目的设置。单击下面的“添加”按钮,在向导中输入被控端计算机的 IP 地址,如图 4.18 所示。

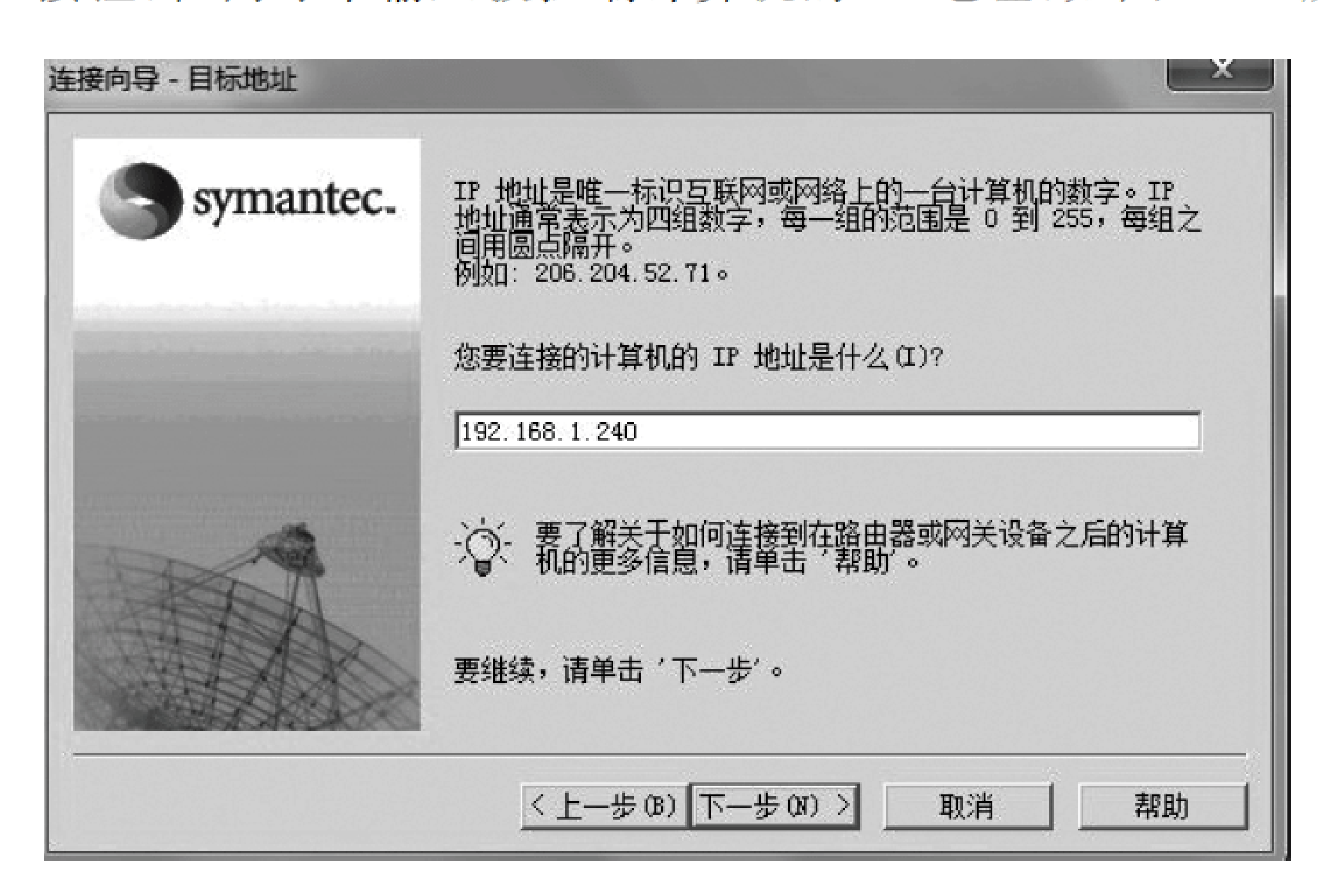


图 4.18 指定被控计算机

单击“下一步”按钮完成控制端的添加,程序提示对名称进行重命名,例如 student。

(2) 右击需要配置的连接项目,选择“属性”,弹出配置窗口。对话框中共有五个选项

卡可供设置。

① 连接信息：设置方式和内容与被控端的设置基本相同，如图 4.19 所示。不同的是主控端只能够选择一种连接方式，同时在选项卡上还可以设置“开始模式”，如其中的“文件传输”复选框，选中之后可以达到与被控端连接时直接进入文件传输界面，而不进入远程操作界面的效果。



图 4.19 连接信息设置

② 设置：用于配置远程连接选项。其中：“要控制的网络被控端 PC 或 IP 地址”填入受控制的远程计算机的主机名或者 IP 地址。设置如图 4.20 所示。

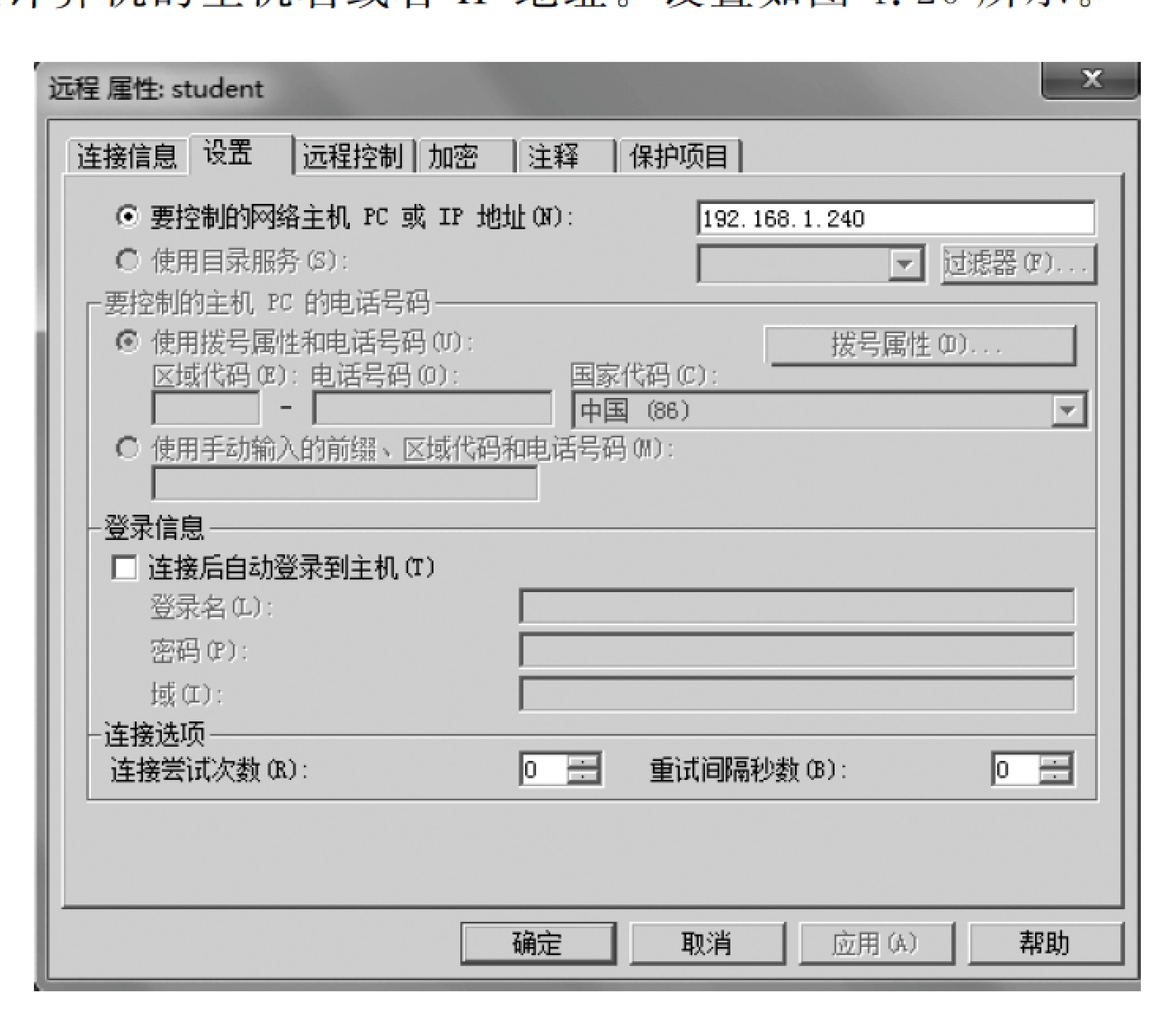


图 4.20 远程控制

- “要控制的主机 PC 的电话号码” 如果远程计算机采用 Modem 拨号呼叫的话，在这里就要填入远程计算机的电话号码，如图 4.20 所示。
- “登录信息”连接后自动登录到被控端，添入完整的登录信息后，就可以保存登录到远程被控端所需的用户账号与密码，而实现自动登录。

其中，192.168.1.240 是被控端的 IP 地址，student 为对方的用户名。

③ 自动化任务：用于设置使用该连接的自动化任务。在 12.5 版本中弱化了这个功能，主要是将远程控制过程中的操作记录下来，在需要的时候回放查看。

④ 安全选项：用于设置主控端在远程控制过程中使用的加密级别，默认是不加密的。可以按自己的需要选择使用对称密钥、公用密钥或 pcAnywhere 加密方式，其中，pcAnywhere 加密方式将前面的两种加密技术结合在一起，具有速度和安全性两方面的优点。

⑤ 保护项目：功能与被控端的设置相同。

(3) 设置完毕后，右击主控端，选择“开始远程控制”，即可自动连接至远程主机的桌面实现安全的桌面远程操作。

作为被控端，在主机中双击新建主机(student)即可，任务栏的右下角会有图标提示。

作为主控端，选中远程中的 student，单击左侧的启动连接或者双击 student，出现如图 4.21 所示界面。用户名就是登录名 teacher，密码就是登录密码 123456。启动远程控制后 pcAnywhere 就开始按照设置的要求尝试连接远端的被控计算机。

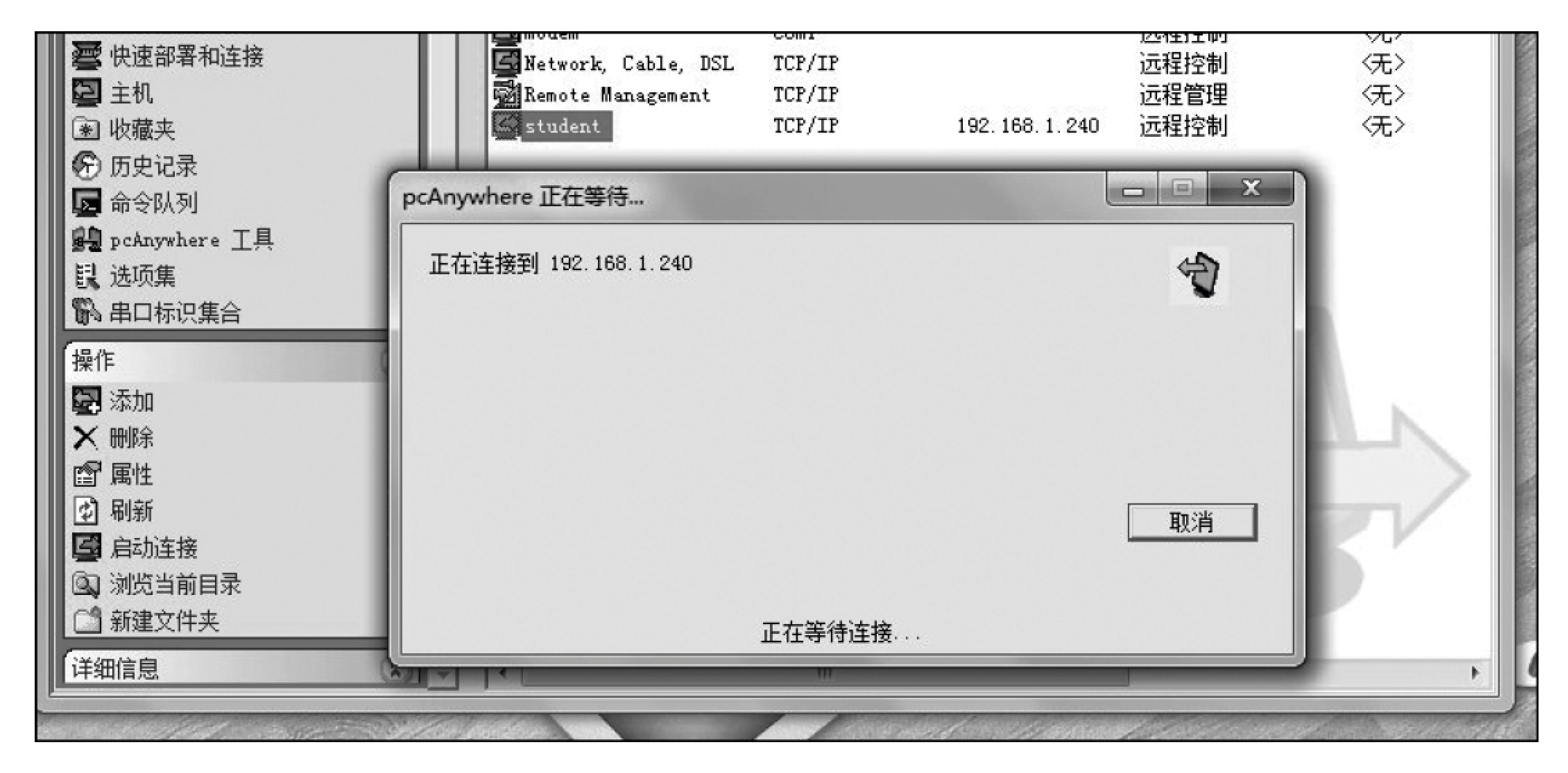


图 4.21 远程连接显示

控制界面如图 4.22 所示，连接成功后将按要求进入远程操作界面或者文件传输界面，可以在远程操作界面中遥控被控计算机。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。

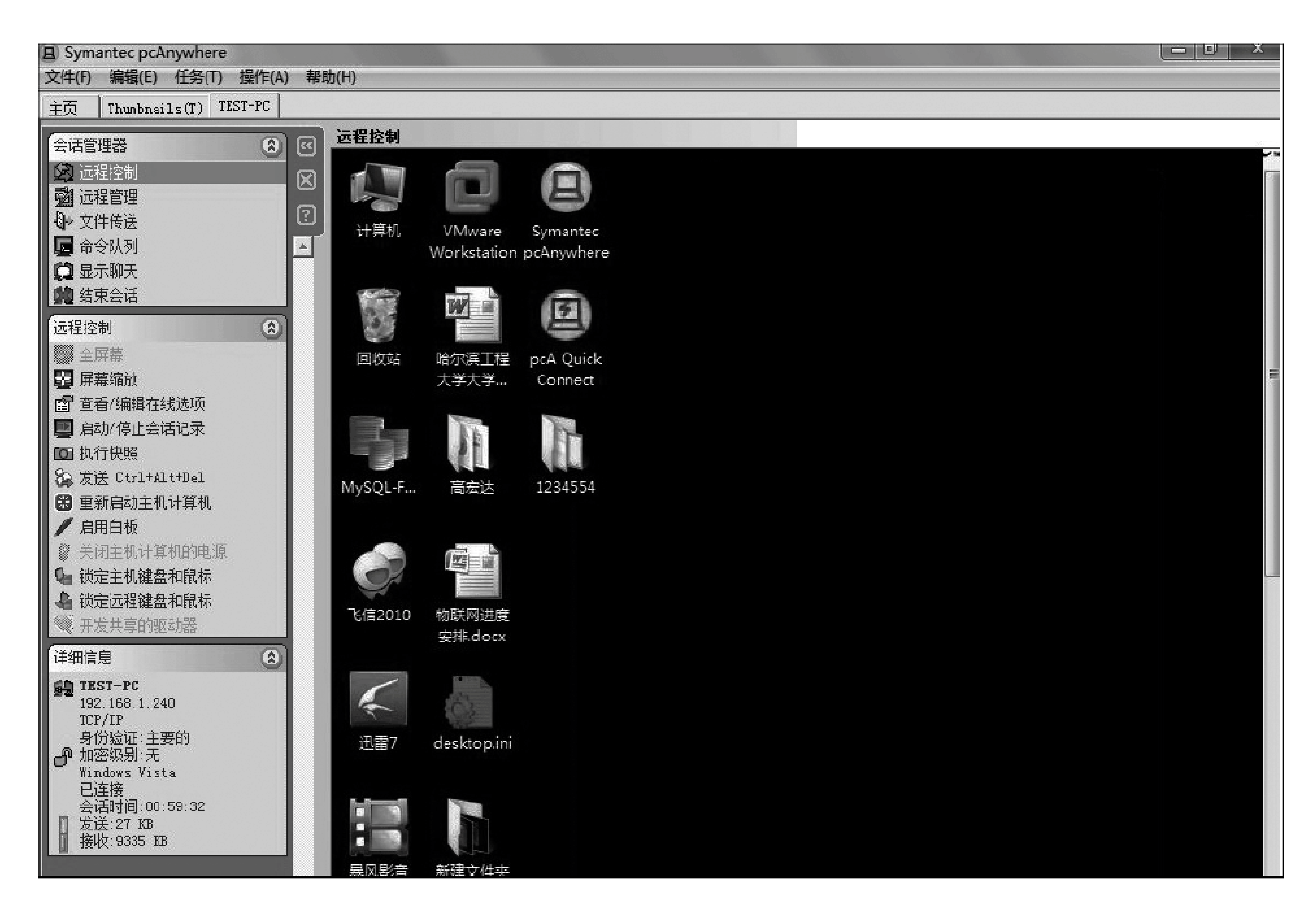


图 4.22 远程控制界面

- 阐述收获与体会。

4.3 扩展实验

实验器材

- pcAnywhere 软件系统 1 套。
- PC(Windows XP/Windows 7)1 台。

预习要求

- 做好实验预习,复习远程控制技术的有关内容。
- 复习 pcAnywhere 软件的操作方法。
- 熟悉实验过程和基本操作流程。
- 做好预习报告。

实验任务

利用 pcAnywhere 软件对远程计算机进行控制。

实验环境

安装 Windows 系统、pcAnywhere 软件(包含被控端和主控端),两台局域网 PC。

实验步骤

任务一:从机(被控端)的 pcAnywhere 基本配置

(1) 通信双方中,一方为“主控端”(主机),另一方为“被控端”(从机)。

(2) 启动从机的 pcAnywhere,在工具栏单击“被控端”,再右击工作区的“NETWORK,

CABLE,DSL”选项,选择“属性”。其中,默认协议设为 TCP/IP,不要更改。

(3) 选择“呼叫者”,在“验证类型”下拉列表中选择 pcAnywhere,右击呼叫者列表,选择新建。

(4) 输入新建用户的登录名和密码(主机呼叫从机时用到),只有拥有此登录名和密码的主机才能呼叫并控制从机。系统默认的权限是主机可完全控制。

(5) 修改被控端的用户登录密码,修改部分系统环境。

任务二:主机(主控端)的 pcAnywhere 基本配置

(1) 启动从机的 pcAnywhere,在工具栏单击“主控端”,再右击工作区的“NETWORK,CABLE,DSL”选项,选择“属性”。其中,默认协议设为 TCP/IP,不要更改。

(2) 选择“设置”,在“控制的网络被控端 PC 或 IP 地址(N):”后输入从机的 IP 地址并单击“确定”按钮。

任务三:远程控制的实施

(1) 运行从机的 pcAnywhere,选择“被控端”,双击“NETWORK,CABLE,DSL”,表示从机现在处于等待状态,随时接受主机的“呼叫”。

(2) 运行主机的 pcAnywhere,选择“主控端”,双击“NETWORK,CABLE,DSL”,程序执行结果因任务二中步骤(2)的设置分两种:

- 若步骤(2)中未设置从机的 IP 地址,则“主控端”自动扫描所有“等待连接”的从机。
- 若步骤(2)中设置了从机的 IP 地址,则显示登录信息,只要用户名和密码通过从机的验证,主机就可顺利取得对从机的控制权,同时在主机屏幕中显示从机的桌面。

任务四:在主机上对从机进行操纵

(1) 单击工具栏中的“改为全屏显示”按钮,可全屏显示从机的桌面而隐藏主机的“开始”菜单和“任务栏”。

(2) 单击工具栏中的“文件传输”按钮,左边显示的是主机资源,右边显示的是从机资源,利用鼠标的拖放功能可实现文件的双机互拷贝。

(3) 单击工具栏中的“查看修改联机选项”按钮,设置锁定从机键盘,单击工具栏中的“结束远程控制对话”按钮。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

第5章　SSL VPN 实验

5.1　SSL VPN 原理

5.1.1　基本概念

随着计算机网络技术和信息技术的发展与应用，越来越多的用户希望能在非正式办公场所享受到单位内部网络的权限和服务，虚拟专用网(virtual private network，VPN)是目前解决这一问题的有效办法。虚拟专用网通过私有的隧道技术在公共数据网络上仿真一条点到点的专线技术。所谓虚拟，是指用户不再需要拥有实际的长途数据线路，而是使用 Internet 公众数据网络的长途数据线路。所谓专用网络，是指用户可以为自己制定一个符合自己需求的网络。利用 VPN 技术构建安全的虚拟私有网络，节省了租用专线的费用。

VPN 技术具有以下优势：

(1) 跨地域的分支机构网络互联互通，构建远程"局域网"，实验资源共享。

(2) 降低网络通信成本，替代昂贵专线。

(3) 信息流畅通，提高效率，业务系统实时信息共享。

(4) 随时随地移动办公，安全接入单位网络。

VPN 技术提供了以下功能：

(1) 用户验证。验证用户身份并严格控制只有授权用户才能访问 VPN。

(2) 地址管理。能够为用户分配专用网络上的地址并确保地址的安全性。

(3) 数据加密。数据经过加密，确保网络其他未授权用户无法读取该信息。

(4) 密钥管理。能够生成并更新客户端和服务器的加密密钥。

(5) 多协议支持。支持公共互联网络上普遍使用的基本协议，包括 IP、IPX 等。

VPN 主要包括 4 项技术：

(1) 隧道技术(tunneling)：隧道是在公网上传递私有数据的一种方式，也是数据包在网络中传输经过的逻辑路径。

(2) 加解密技术(encryption & decryption)：保证数据传输过程中的安全。

(3) 密钥管理技术(key management)。

(4) 使用者与设备身份认证技术(authentication)：保证 VPN 通信方的身份确认及合法。

目前，常用的 VPN 技术主要有三种：IPSEC(Internet protocol security)、SSL(secure socket layer)、MPLS(multiProtocol label switch)(电信运营商提供)。

5.1.2　SSL VPN

将安全套接层协议(secure socket layer，SSL)和 VPN 组合，称为基于 SSL 的 VPN，

简称 SSL VPN。SSL VPN 作为一种价格便宜、安装方便同时具有完善的远程访问功能的安全方案,在保险业、银行、金融、证券行业、电信行业的无线网络等方面的应用越来越广泛。安全性是 SSL VPN 的一个重要特性,它也是设计和维护的重点内容。

SSL 协议是网景公司设计的基于 Web 应用的安全协议,它指定了在应用程序协议(如 HTTP、Telnet 和 FTP 等)和 TCP/IP 协议之间进行数据交换的安全机制,为 TCP / IP 连接提供数据加密、服务器认证以及可选的客户机认证。SSL 协议是由 SSL 记录协议、握手协议、密钥更改协议和告警协议组成,它们共同为应用访问连接提供认证、加密和防篡改等功能。其工作流程如图 5.1 所示。

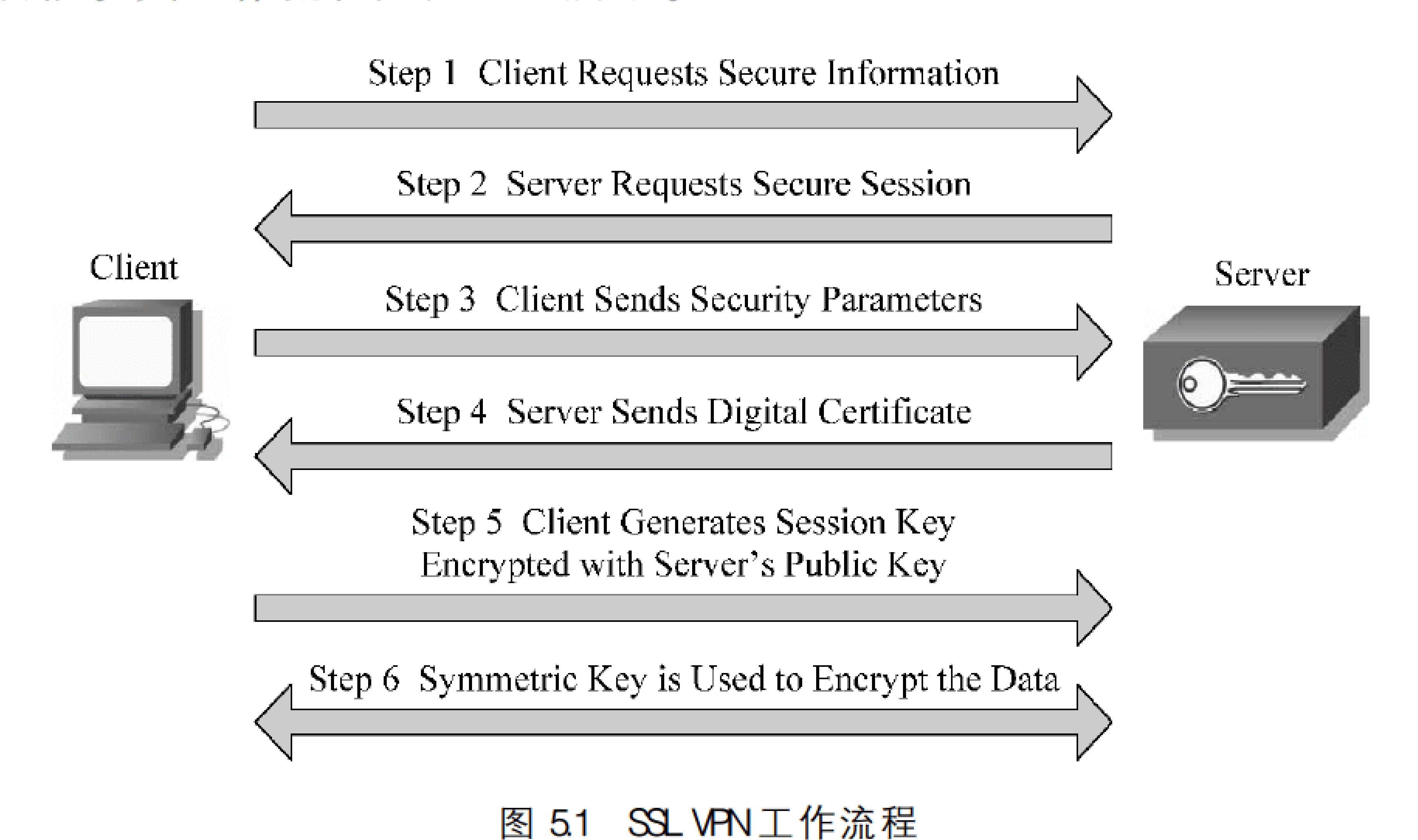


图 5.1 SSL VPN 工作流程

SSL VPN 的一般实现方式是在企业的防火墙后面放置一个 SSL 代理服务器, SSL 代理服务器将提供一个远程用户与各种不同的应用服务器之间的连接,主要有握手协议、记录协议、警告协议的通信。SSL VPN 的通信过程主要集中在握手协议上,过程如下:

(1) SSL 客户机连接到 SSL 服务器,并要求服务器验证身份。

(2) 服务器发送数字证书证明自身的身份。这个交换包括整个证书链,直到某个证书颁发机构(CA)通过检查有效日期并确认证书包含可信任 CA 的数字签名来验证证书的有效性。

(3) 服务器发出一个请求,对客户端的证书进行验证。

(4) 双方协商加密算法和用于完整性检查的 Hash 函数,通常由客户端提供它所支持的所有算法列表,然后由服务器选择其中最健壮的加密算法。

(5) 客户机和服务器通过下列步骤生成会话密钥:

① 客户机生成一个随机数,并使用服务器的公钥对它加密,再送到服务器。

② 服务器用客户机的公钥加密,发送至客户机以表示响应。

③ 使用 Hash 函数从随机数据中生成密钥。

SSL VPN 技术的主要特点如下:

- 客户端维护简单。
- 提供增强的远程安全接入功能。
- 提供更细粒度的访问控制。

- 能够穿越防火墙等设备。
- 能够较好地抵御外部病毒攻击。
- 网络部署方便灵活。

SSL VPN 的四种工作模式如下。

(1) 代理：HTTP proxy。

(2) 应用转换：把 C/S 应用客户端转化成 Web 方式。

(3) 端口转发：对任意的 C/S 应用实现 SSL 保护。

(4) 网络连接(NC mode)：用 SSL 实现网络层的连接。

5.2 VPN 配置实验

实验器材

- PC(Windows XP/Windows 7)1 台。

预习要求

- 做好实验预习，复习 VPN 及隧道技术的有关内容。
- 复习 Windows 操作系统的网络设置方法。
- 熟悉实验过程和基本操作流程。
- 做好预习报告。

实验任务

通过本实验，掌握 VPN 服务器搭建技术。

实验环境

装有 Windows XP 操作系统的 PC。

预备知识

- VPN 技术及原理。
- 隧道技术。

实验步骤

1. 基础环境配置

开启 Windows XP 系统自带的防火墙系统(Windows firewall/Internet connection sharing(ICS))(需要允许 1723 端口通过)。

必须开启的服务包括远程注册表服务(Remote Registry)、Server 服务(Server)、Router 路由服务(Routing and Remote Access)，如图 5.2 所示。

2. 启动系统服务

默认情况下所需服务中，远程注册表服务(Remote Registry)和 Server 服务(Server)是自动启动的，只有 Router 路由服务(Routing and Remote Access)默认禁止。右击桌面上的“我的电脑”，选择“管理”选项，进入“计算机管理”后，单击左侧的“服务和应用程序”，选择“服务”选项，如图 5.2 所示，在右侧找到 Routing and Remote Access，右击，选择“属

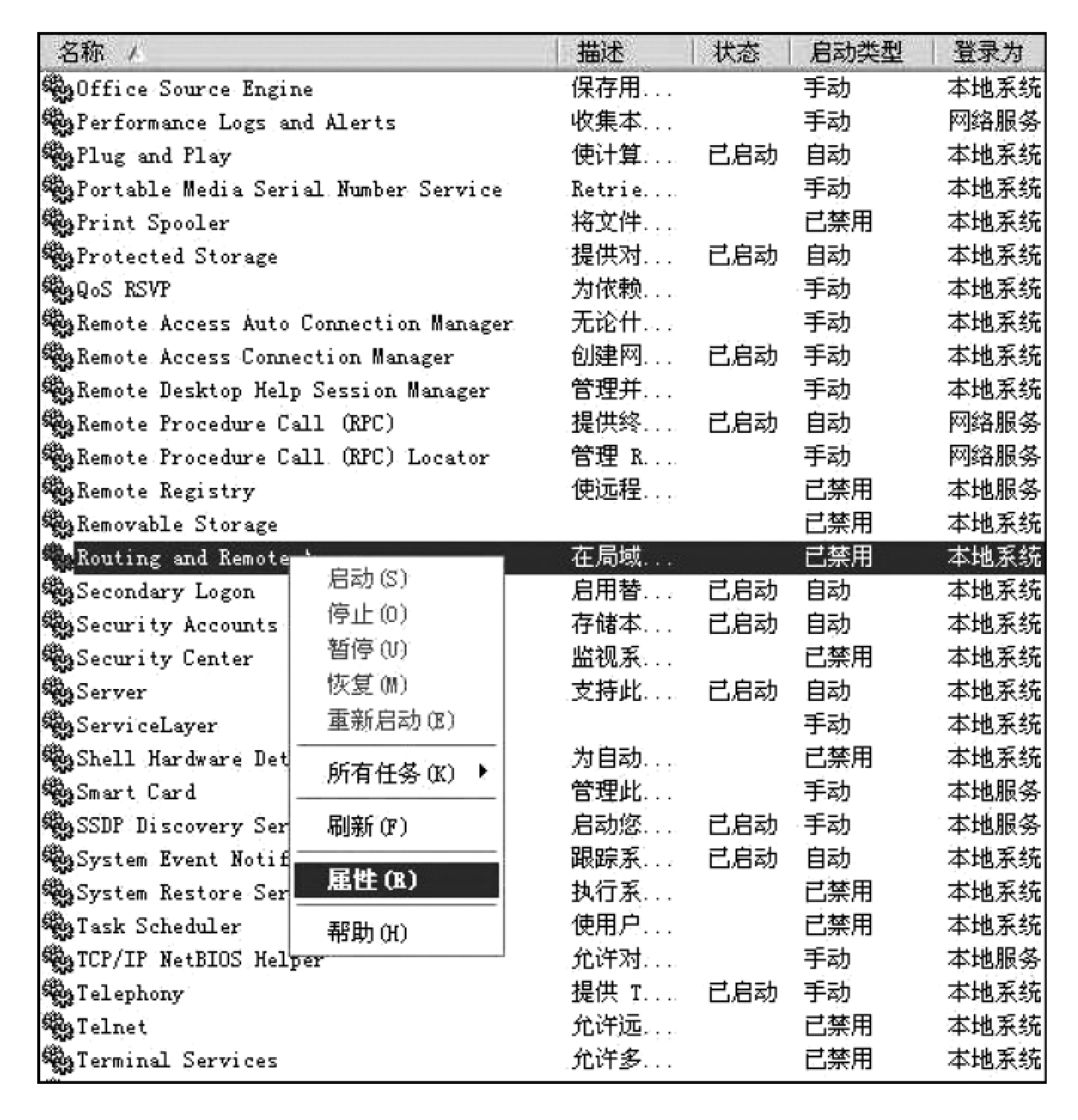


图 52　系统服务界面

性”选项，更改“启动类型”为“自动”，然后单击“确定”按钮。所有设置完成后，右击 Routing and Remote Access，单击“启动”按钮。

右击“网上邻居”，选择“属性”选项，进入“网络连接”，会发现增加了一个“传入的连接”，如图 5.3 所示。



图 53　传入的连接界面

右击“传入的连接”，选择“属性”选项，在“常规”选项卡中，选中“允许他人通过 Internet 或其他网络以‘隧道操作’方式建立到我的计算机的专用连接(W)”复选框，如图 5.4 所示。

单击“用户”选项卡，单击下面的“新建(N)...”按钮建立一个用户名和密码，也可以选中已有的用户名和密码。到“网络”选项卡中，单击“安装(I)...”按钮，在“协议”选择包含“NWLink IPX/SX/NetBIOS 协议”后，单击“确定”按钮，如图 5.5 所示。



图 5.4 VPN连接设置界面

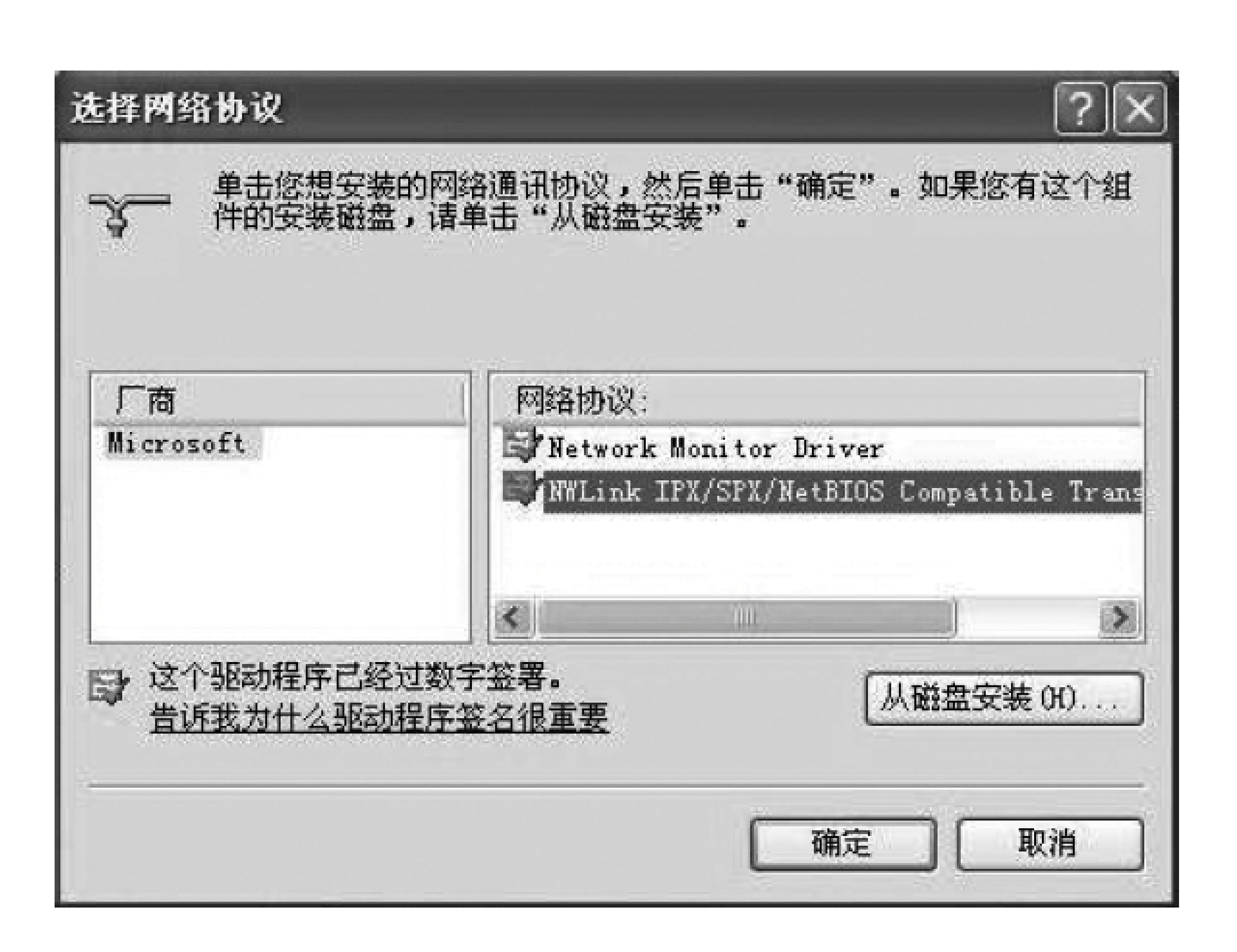


图 5.5 协议安装界面

如果 VPN 服务器所在的网络没有开启自动获取 IP 地址(DHCP)，则需要配置传入连接的 IP 范围，双击“Internet 协议(TCP/IP)”，在弹出的窗口中选择“指定 TCP/IP 地址”，并填写与 VPN 服务器同一网段的空闲地址，推荐为双数，如图 5.6 所示。

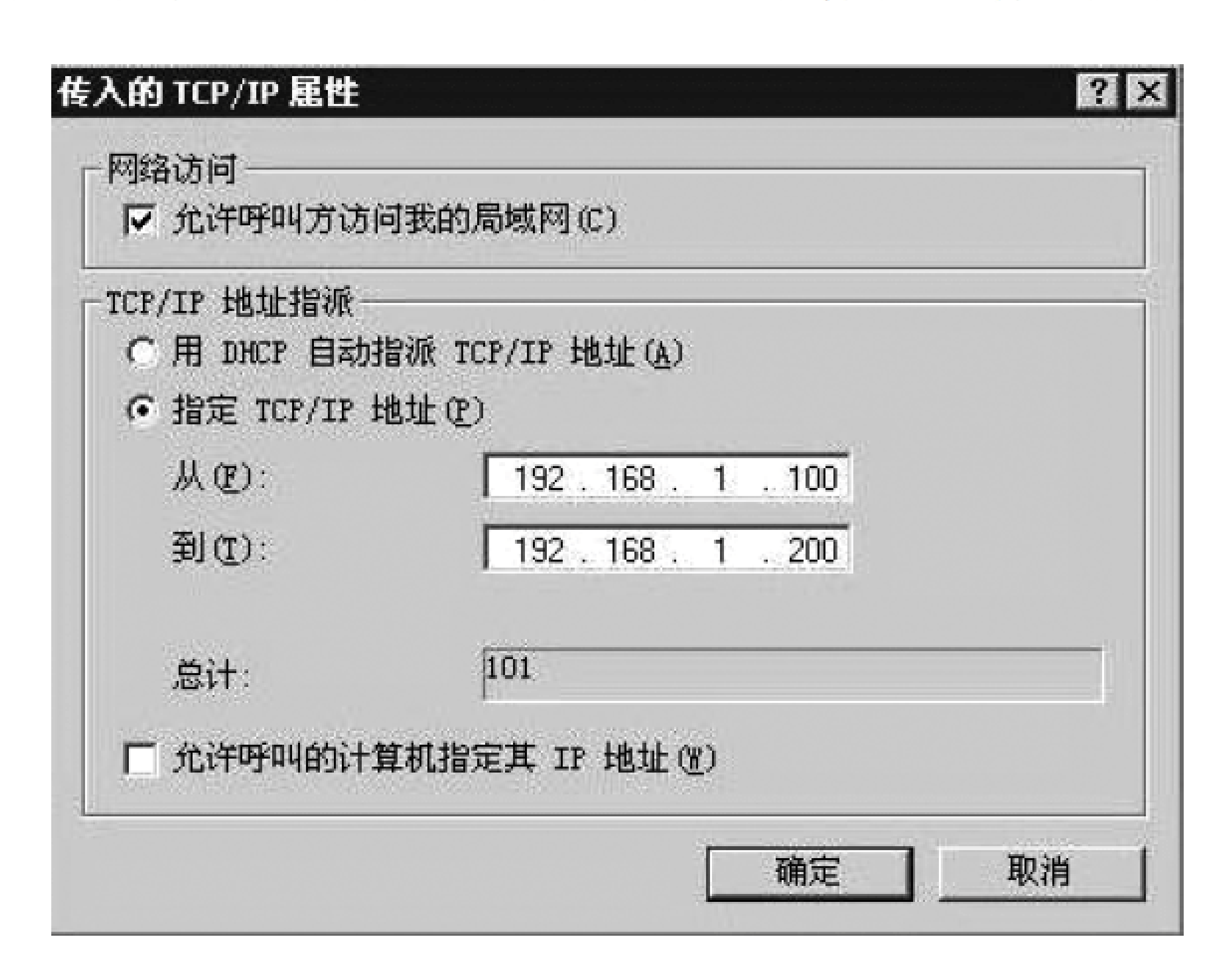


图 5.6 IP地址范围设置界面

3. 客户端(接入端)的相关配置

打开“网络连接”，单击左侧“网络任务”下的“创建一个新的连接”。在打开的“新建连

接向导”中单击“下一步”按钮，“网络连接类型”选择“连接到我的工作场所的网络”；单击“下一步”按钮，选择“虚拟专用网络连接”；单击“下一步”按钮，填写“公司名”，可以留空不写(留空为：虚拟专用网络)；单击“下一步”按钮，填写 VPN 服务器的 IP 地址或域名，如图 5.7 所示；单击“下一步”按钮，在出现的完成页面中单击“完成”按钮。

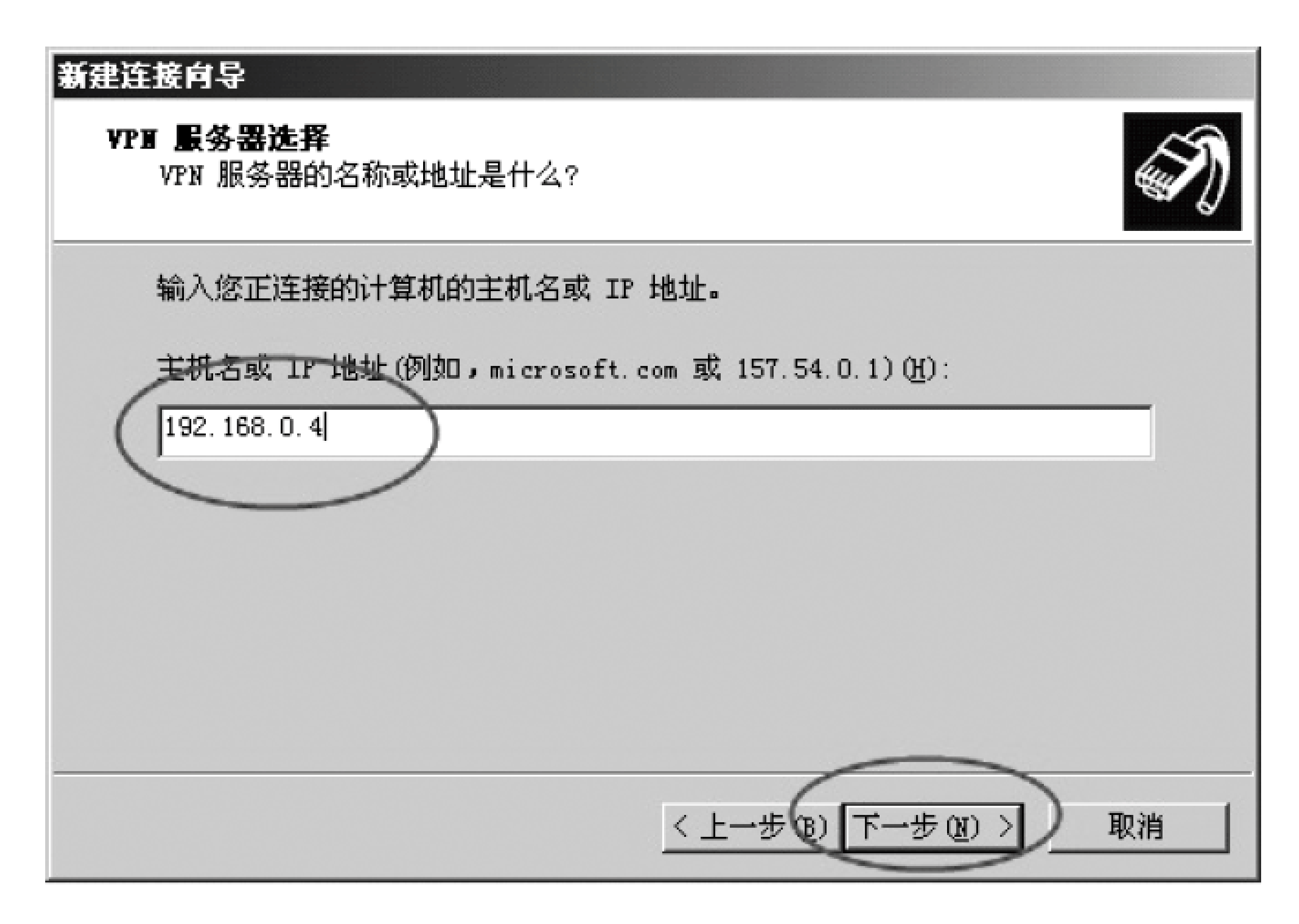


图 5.7　VPN 服务器的 IP 地址设置界面

4. VPN 使用设置

打开刚刚创建好的连接，输入允许接入的用户名和密码，单击“连接”按钮，客户机成功接入 VPN 服务器。通过查看连接属性，可以看到时间、流量等信息，如图 5.8 所示。

使用 XP 系统做 VPN 服务器只能同时允许一个用户接入，如果有其他用户接入，会出现如图 5.9 所示错误。

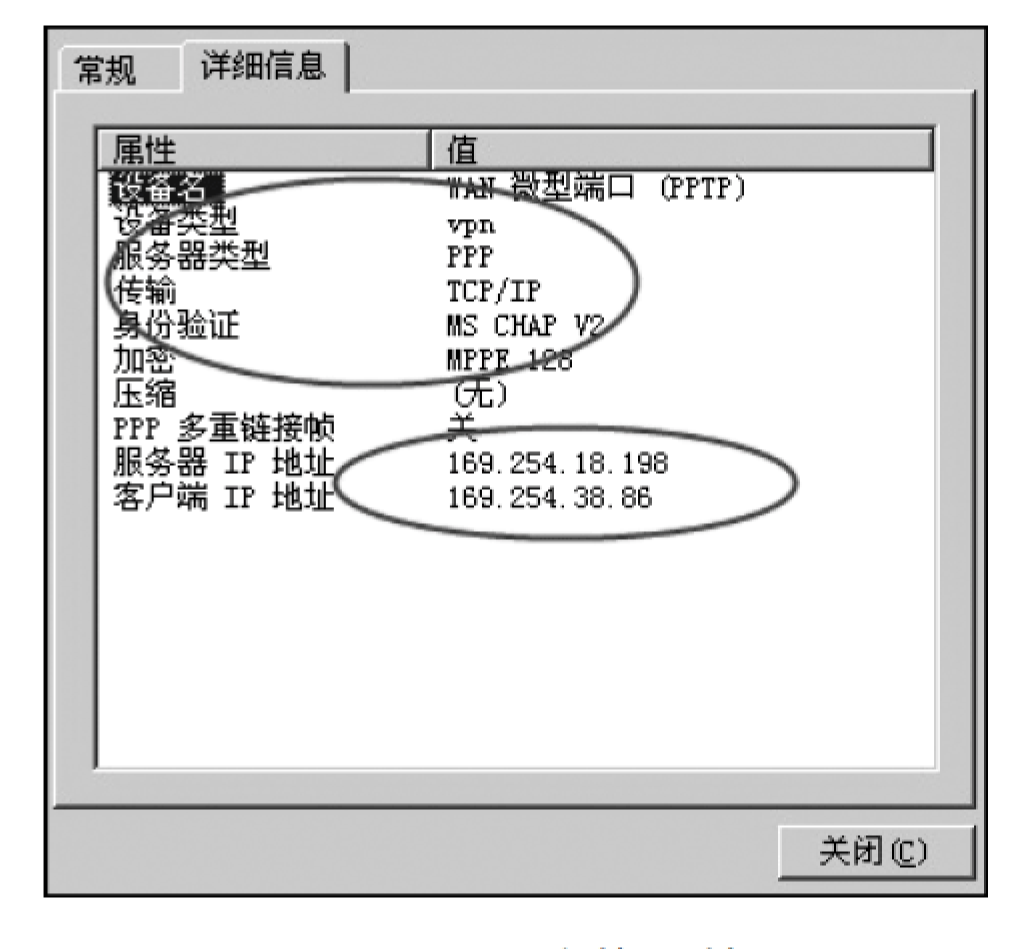


图 5.8　VPN 连接属性

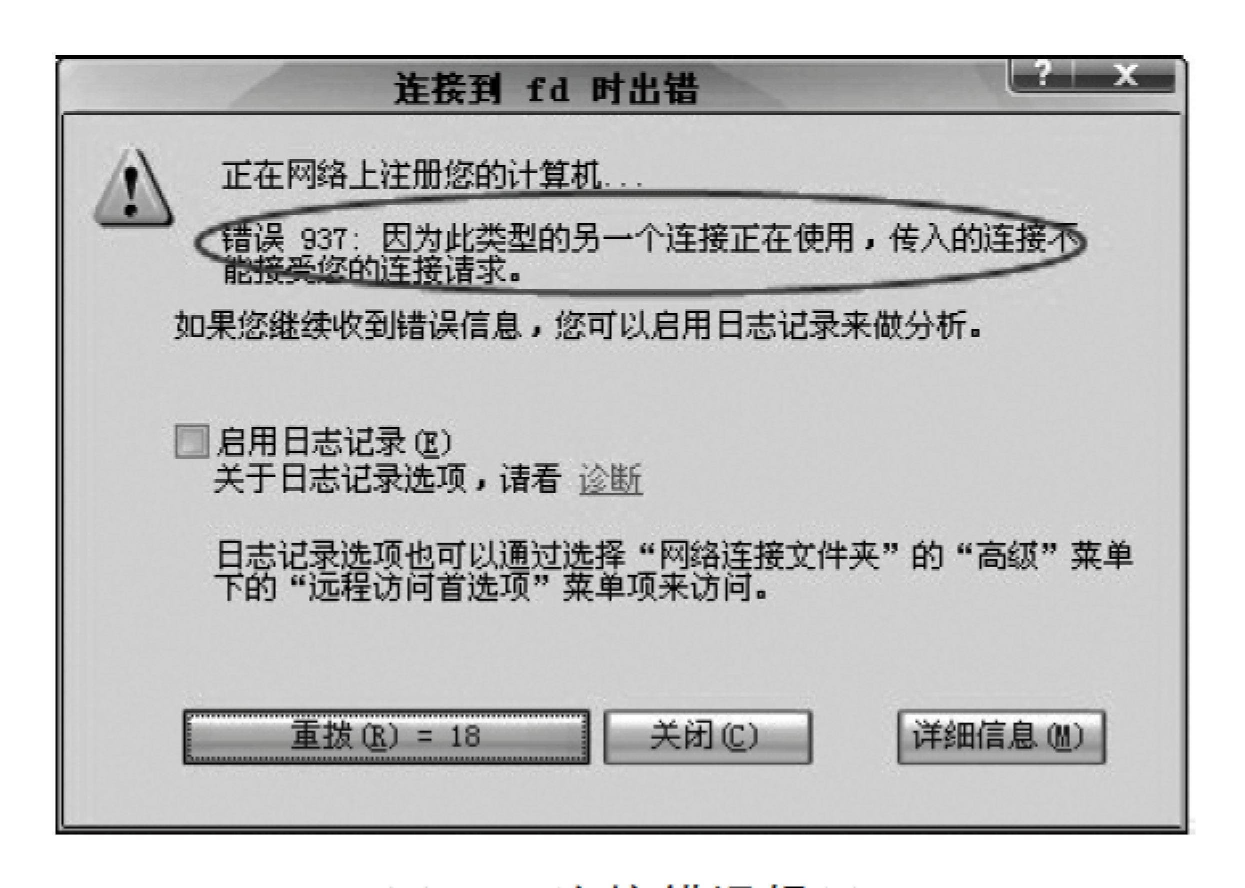


图 5.9　连接错误提示

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。

• 阐述收获与体会。

思考题

为什么要添加“NWLink IPX 协议”?

5.3　SSL VPN 配置实验

实验器材

• OpenVPN 软件系统 1 套。
• PC(Windows XP/Windows 7)1 台。

预习要求

• 做好实验预习,复习 SSL VPN 的有关内容。
• 复习 OpenVPN 的使用方法。
• 熟悉实验过程和基本操作流程。
• 做好预习报告。

实验任务

通过本实验,掌握 VPN 服务器搭建技术。

实验环境

装有 Windows 7 操作系统的 PC。

预备知识

• VPN 技术及原理。
• 隧道技术。

实验步骤

1. 服务器端配置

需要注意的是:在 Client 端和 Server 端需要使用相同版本的 OpenVPN,本实验使用的软件版本是 OpenVPN 2.1.4。在 Windows 7 操作系统下采取默认安装,直至完成即可,如图 5.10 所示,安装目录为 C:\Program Files\OpenVPN。

具体配置工作如下。

(1) 修改 easy-rsa 目录下的 vars.bat.sample 内容,用写字板打开,并将其改名为 vars.bat。原内容如下:

• set KEY_COUNTRY=US
• set KEY_PROVINCE=CA
• set KEY_CITY=SanFrancisco
• set KEY_ORG=OpenVPN
• set KEY_EMAIL=mail@host.domain

根据自身情况修改,也可以不修改。可以改为:

• set HOME=C:\Program Files\OPENVPN\easy-rsa　　　//新增

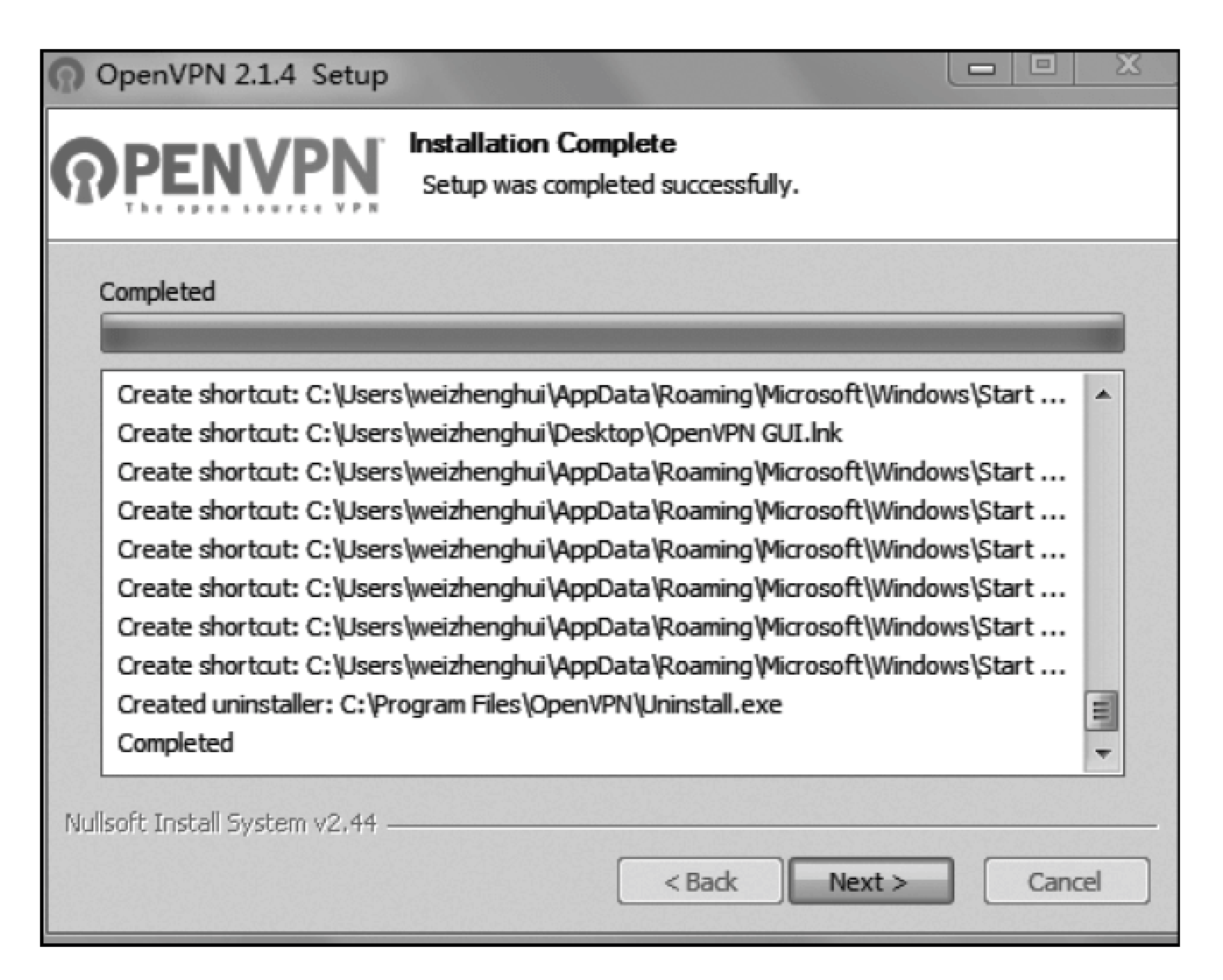


图 5.10 OpenVPN 安装界面

- set KEY_COUNTRY=CN　　　　　　　　　　//(国家)
- set KEY_PROVINCE=HLJ　　　　　　　　　//(省份)
- set KEY_CITY=hrbeu　　　　　　　　　　//(城市)
- set KEY_ORG=OpenVPN　　　　　　　　　//(组织)
- set KEY_EMAIL=mail@host.domain　　　　//(邮件地址)

(2) 把 C:\Program Files\OpenVPN\easy-rsa 中的 openssl.cnf.sample 改为 openssl.cnf。在 DOS 环境下运行：进入目录 C:\Program Files\OpenVPN\easy-rsa。分别输入 vars 和 clean-all.bat 命令。

(3) 生成根 CA，输入命令：build-ca.bat，如图 5.11 所示。

```
C:\Program Files\OpenVPN\easy-rsa>build-ca.bat
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....................++++++
...................................++++++
writing new private key to 'keys\ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:_
```

图 5.11 build-ca.bat 运行界面

输入系统环境信息和服务器基本信息，包括组织结构名称、国家、服务器名称、使用者信息等内容，如图 5.12 所示。

输入：build-dh.bat，完成基本设置，如图 5.13 所示。

(4) 生成服务器端证书、客户端证书、TA 证书。服务器端证书、TA 证书必须生成在服务器端机器上；客户端证书、TA 证书必须生成在客户端机器上。首先，生成服务器端 Server 使用的证书，输入命令：build-key-server.bat server，如图 5.14 所示。

```
Country Name (2 letter code) [CN]:CN
State or Province Name (full name) [HLJ]:HLJ
Locality Name (eg, city) [HeiLongJiang]:HeiLongJiang
Organization Name (eg, company) [OpenVPN]:OpenVPN
Organizational Unit Name (eg, section) []:
Locality Name (eg, city) [HeiLongJiang]:HeiLongJiang
Organization Name (eg, company) [OpenVPN]:OpenVPN
Organizational Unit Name (eg, section) []:wyz group
Common Name (eg, your name or your server's hostname) []:wyz group
Email Address [mail@host.domain]:mail@host.domain

C:\Program Files\OpenVPN\easy-rsa>
```

图 5.12　服务器基本信息设置界面

```
C:\Program Files\OpenVPN\easy-rsa>build-dh.bat
Loading 'screen' into random state - done
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
```

图 5.13　build-dh.bat 运行界面

```
C:\Program Files\OpenVPN\easy-rsa>build-key-server.bat server
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.............++++++
.................++++++
writing new private key to 'keys\server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
```

图 5.14　build-key-server.bat 运行界面

输入必要的注册信息：An optional company name []:wyzz，这些信息都是之前定义好的，密码处留空，以后可以进行设置，如图 5.15 所示。最后出现提示信息“Sign the certificate ? [y/n]”，输入：y。

生成 Client 证书，输入命令：C:\Program Files\OpenVPN\easy-rsa>build-key.bat client，如图 5.16 所示。

如前所述，输入必要的注册信息。密码同样留空不写，输入：wyzz，最后出现提示信息“Sign the certificate? [y/n]”，输入：y。

完成 ta.key 文件的生成，即 C:\Program Files\OpenVPN\easy-rsa>openvpn--genkey--secret keys/ta.key。所有的根 CA、服务器、客户端所需证书和密钥文件准备就绪后，设置配置文件。利用 build-key client2 可以继续配置第二个 VPN 客户端密钥，配置方法同上。

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:wyzz
Using configuration from openssl.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'HLJ'
localityName          :PRINTABLE:'HeiLongJiang'
organizationName      :PRINTABLE:'OpenVPN'
organizationalUnitName:PRINTABLE:'wyz group'
commonName            :PRINTABLE:'wyz test'
emailAddress          :IA5STRING:'mail@host.domain'
Certificate is to be certified until Dec  5 09:51:34 2020 GMT (3650 days)
Sign the certificate? [y/n]:
```

图 5.15 注册信息界面

```
C:\Program Files\OpenVPN\easy-rsa>build-key.bat client
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
..............................................++++++
.........................................................................+++++
+
writing new private key to 'keys\client.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
```

图 5.16 build-key.bat 运行界面

(5) 服务器端配置。服务器的配置文件在 C:\ProgramFiles\OpenVPN\sample-config 中。server. ovpn 内容如下:

```
port 1194                                 //1194 端口进行通信
;proto tcp
proto udp
;dev tap                                  //虚拟设备型号
dev tun
;dev-node MyTap
ca ca.crt
cert server.crt
key server.key # This file should be kept secret
dh dh1024.pem
//服务器端要用的证书
server 10.8.0.0 255.255.255.0
//服务网关的虚拟网段
…
```

将生成的 ca. crt、dh1024. pem、server. crt、server. key 和配置文件 server. ovpn 复制到 C:\Program Files\OpenVPN\config 目录下,这五个文件是 VPN 服务器端运行所必需的文件。

（6）客户端文件配置。客户端 client.ovpn 的配置文件在 C:\ProgramFiles\OpenVPN\sample-config.client.ovpn 内容中：

```
remte my- server- 1 1194
;remte my- server- 2 1194
```

更改如下：

```
remote 192.168.1.233 1194
;remote 192.168.1.233 1194
```

客户端所需证书及其密钥：

```
# file can be used for all
ca ca.crt
cert client.crt
key client.key
```

将生成的 ca.crt、client.crt、client.key、ta.key 和配置文件 client.ovpn 复制到 C:\Program Files\OpenVPN\config 目录下，这五个文件是 VPN 客户端运行所必需的文件。配置结束，在右下角会有图标显示，红色为未连接，黄色为等待连接，绿色为连接成功。

2. 客户端连接设置

（1）Server 端配置：双击系统的“控制面板”，选择“网络”选项，再选择“Internet\网络连接”选项，如图 5.17 所示。



图 5.17 系统网络连接界面

按 Alt 键，会出现“文件”等菜单栏，选择“文件”|“新建传入连接”命令，添加用户。为客户端输入用户名和密码等信息，如图 5.18 所示。



图 5.18 添加用户界面

单击“下一步”按钮,选择“通过 Internet”,单击“允许访问”。创建连接,为客户端授权即可。设置结束后,在网络连接中会出现新接入的连接图标。

(2) Client 端配置:双击“控制面板”,选择“网络”,进入“Internet\网络连接”界面,设置新的链接或网络。选择“连接到工作区”。在“你想如何连接?”选项中选择首项“是我的 Internet 连接(VPN)”。

在 Internet 地址中填入 Server 端 IP 地址,如图 5.19 所示,填入授权的用户名和密码,即先期创建的账号和密码。



图 5.19 客户端配置界面

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

第 6 章　防火墙实验

6.1　防火墙技术

防火墙是一类防范措施的总称。所谓“防火墙”，是指一种将内联网和公众访问网(外联网 Internet)分开的方法，它使得内联网与外联网互相隔离，限制网络互访来保护内部网络。它是一个或一组由软件和硬件构成的系统，在两个网络通信时执行的一种访问控制尺度，防止重要信息被更改、复制、毁坏。设置防火墙的目的是为了在内部网与外部网之间设立唯一的通道，简化网络的安全管理。

6.1.1　基本概念

防火墙是一个网络安全专用词，它是在内部网(或局域网)和互联网之间，或者是内部网的各部分之间实施安全防护的系统，通常由硬件设备(路由器、网关、堡垒主机、代理服务器)和防护软件等共同组成。在网络中它可对信息进行分析、隔离、限制，从而保护网络安全运行。

防火墙的体系结构主要包括如下几个部分。

(1) 屏蔽路由器(screening router)：它是防火墙最基本的构件，可以由路由器实现，也可以用主机实现。屏蔽路由器作为内外连接的唯一通道，要求所有报文都必须在此通过检查。

(2) 双穴主机网关(dual homed gateway)：这种配置是用一台装有两块网卡的堡垒主机做防火墙。其两块网卡各自与受保护网和外部网相连，其防火墙软件可以转发应用程序、提供服务等。

(3) 被屏蔽主机网关(screened host gateway)：屏蔽主机网关易于实现也很安全，应用广泛。网关的基本控制策略由安装在上面的软件决定。

(4) 被屏蔽子网(screened subnet)：这种方法是在内部网络和外部网络之间建立一个被隔离的子网，用两台分组过滤路由器将这一子网分别与内部网络和外部网络分开。

防火墙具有以下作用：

(1) 取消或拒绝任何未被明确允许的软件包通过。

(2) 将外部用户保持在内部网之外，对外部用户访问内部网做出限制。

(3) 强制执行注册、审计和报警等。

6.1.2　个人防火墙

主流的个人防火墙包括天网防火墙、诺顿防火墙、江民防火墙、金山网镖和瑞星个人防火墙。

6.1.2.1 天网防火墙

天网防火墙是由天网安全实验室研发制作的、应用于个人计算机的网络安全工具。它根据系统管理者设定的安全规则(security rules)防护网络,提供强大的访问控制、应用选通、信息过滤等功能,能够抵挡网络入侵和攻击,防止信息泄露,保障用户机器的网络安全。天网防火墙把网络分为本地网和互联网,可以针对来自不同网络的信息,设置不同的安全方案。

天网防火墙具有以下特征:

(1) 严密的实时监控。防火墙会监控来自外部的安全威胁,过滤掉所有未授权的连接,时刻保护系统安全。

(2) 灵活的安全规则。通过防火墙的规则设置面板,可以方便地对防火墙规则进行增加、删除和修改,可以根据自身需要去制定相应的规则,官方会根据网络安全环境不定时升级最新规则库。

(3) 便利的应用程序规则设置。拒绝任何未经授权的内部程序连接网络,从而阻断所有病毒木马泄露秘密信息。

(4) 详细的访问记录和完善的报警系统。遇到安全威胁即发出报警,并记录下攻击来源及其攻击类型等信息,在第一时间掌握系统的安全情况。

(5) 独创的扩展安全级别。无需对防火墙进行繁琐设置,只要把安全级别调成“扩展”级别即可,每当有最新规则,防火墙会自动联网升级。

(6) 完善的密码保护措施。查看、修改、关闭防火墙均需要提供密码,防止病毒或黑客恶意关闭防火墙以制造安全漏洞。

(7) 稳定的进程保护。进程保护可以使防火墙的进程享受超越系统级的安全待遇,保护防火墙的进程不被恶意关闭。

(8) 智能的入侵检测。针对密集的攻击,天网防火墙会自动判断并将攻击源加入列表,默认该攻击源。一旦攻击源被加入默认列表,所有来自这里的攻击一律屏蔽。

6.1.2.2 诺顿防火墙

诺顿防火墙是由赛门铁克公司提供的一款功能强大的防火墙。诺顿防火墙所集成的功能相当丰富,除了作为基础的防火墙功能,入侵检测、隐私保护等功能也颇为强大。诺顿在浏览器中集成了增加 Web 辅助功能的插件,该插件可以动态地根据所浏览网站的情况进行弹出广告窗口、Applet、ActiveX 等内容的阻塞,而用户可以针对单个网站决定是否阻塞这些内容,同时以关键字的形式维护广告信息过滤清单。另外,该插件还可以帮助用户禁止将浏览器信息、访问历史信息等泄露给外部网络。诺顿防火墙所集成的入侵检测组件带有大量的攻击指纹,能够设定在规定时间内阻止发起的攻击,其功能性已经趋近于专业的入侵检测系统。

诺顿的定制能力不单体现在对防火墙规则的设定上,辅助功能组件的管理功能也相当强大。以入侵检测指纹为例,用户可以决定哪些攻击需要被检测,而哪些需要被忽略;同时,可以选择发现攻击时的告警方式。另外,不只防火墙具有防护等级,包括隐私保护等辅助功能也可以独立设置级别,用户可以快速简便地设定计算机的防护强度。

在整体设计上诺顿相当规整，大量的功能很好地排布在几个选项中，相应的许多操作需要深入多个界面才能完成，这也是诺顿操作负担较高的主要原因。诺顿为用户提供了多种应用情境模式的选择，对这些模式分别赋予了不同的规则权限。初级用户可以安全高效地利用模式的切换来调整对计算机的保护，而相对专业的基于地址和协议的过滤条件设定被隐藏在了高级设置部分，专业用户在需要的情况下可以通过该界面定义更加复杂的防护策略。

6.1.2.3 江民防火墙

江民防火墙是一款专为解决个人用户上网安全而设计的免费网络安全防护工具，产品融入了先进的网络访问动态监控技术，彻底解决黑客攻击、木马程序及互联网病毒等各种网络危险的入侵，全面保护个人上网安全。

江民防火墙具有以下特征：

(1) 全新网络访问动态监控技术。动态监控黑客攻击、木马程序、互联网病毒等危险，保护上网账号、QQ 密码、游戏分值、银行账号、邮件密码、个人隐私等重要信息不外泄。

(2) 网络安全级别设定，智能防黑客、拦木马。高、中、低、自定义四种安全级别设定满足不同需求用户网络安全选择；监视网络数据流，遇危险，报警提示。

(3) 程序访问控制技术，网络日志记录技术。用户可对本地网络规则进行匹配设置，保证只有安全可靠的访问才被允许；详细记录网络链接情况，留下非法访问和未被授权访问对象详细的 IP 地址。

(4) 网络访问控制，过滤不良网站，保证数据安全。通过设置防火墙管理中的区域访问控制规则，可以阻止不良网站和受控制网段访问计算机，清洁网络空间，保证数据安全。

6.1.2.4 金山网镖

金山网镖是一款由金山毒霸推出，为个人计算机量身定做的网络安全产品。它根据个人上网的不同需要，设定安全级别，有效地提供网络流量监控，应用程序访问网络权限控制，病毒预警，黑客、木马攻击监测。

金山网镖具有以下特征：

(1) 全面安全防护。金山网镖是专业的个人网络防火墙，提供对黑客程序、木马和间谍软件以及其他恶意程序的拦截查杀，对网络进行全方位攻击防护，并且，还提供了网络访问监控、共享目录管理、不良网站过滤等多种网络安全实用功能。

(2) 防网络钓鱼。防止钓鱼网站、钓鱼邮件的攻击，用户访问钓鱼网站时网镖会自动拦截，防止用户的账号、密码等重要信息被盗。

(3) 历史痕迹清理。帮助用户预览并清理软件使用的痕迹，避免重要文件、信息或个人隐私被泄露。

(4) 木马防火墙。通过多种技术，实现对木马进程的查杀。系统中一旦有木马、黑客或间谍程序访问网络，会及时拦截该程序对外的通信访问，然后对内存中的进程进行自动查杀，保护用户网络通信的安全。这对防御盗取用户信息的木马、黑客程序特别有效。具体体现在以下三个方面：①能够设置应用程序的访问权限；②通过高、中、低三种安全级

别的设定，达到不同程度地保护用户安全的目的；③能够阻止如冰河、B10、网络神偷等常见木马对用户的危害；若有木马侵入，金山网镖会及时拦截，并弹出对话框告知用户已成功拦截，真正做到实时保护计算机的目的。

(5) 智能防黑技术。融杀毒技术与网络防火墙技术于一体，直接查杀流行木马与黑客程序。动态监视计算机的 Internet 活动状态，随时加以控制。高级用户可以完全细致地定制不同的 IP 包过滤规则。

(6) 程序应用规则中可以根据自己的需要设置各程序访问互联网和局域网的权限，一般来说，很多程序是可以设置成禁止访问网络来减小受攻击的可能程度。

6.1.2.5 瑞星防火墙

瑞星个人防火墙最新版采用增强型指纹技术，有效地监控网络连接；内置细化的规则设置，使网络保护更加智能；游戏防盗、应用程序保护等高级功能，为个人计算机提供全面安全保护；通过过滤不安全的网络访问服务，极大地提高了用户计算机的上网安全；彻底阻挡黑客攻击、木马程序等网络危险，保护上网账号、QQ 密码、网游账号等信息不被窃取。

瑞星防火墙具有以下特征：

(1) 防火墙多账户管理。防火墙提供“管理员”和“普通用户”两种账户。防火墙提供切换账户功能可以在两种账户之间进行切换。管理员可以执行防火墙的所有功能；普通用户不能修改任何设置、规则，不能启动/停止、退出防火墙。

(2) 未知木马扫描技术。通过启发式查毒技术，当有程序进行网络活动的时候，对该进程调用未知木马扫描程序进行扫描，如果该进程为可疑的木马病毒，则提示用户。此技术提高了对可疑程序自动识别的能力。

(3) IE 功能调用拦截。由于 IE 提供了公开的 Com 组件调用接口，有可能被恶意程序所调用。此功能是对需要调用 IE 接口的程序进行检查。如果检查为恶意程序，向用户报警。

(4) 反钓鱼、防木马病毒网站。反钓鱼、防木马病毒网站提供强大的、可以升级的黑名单规则库，库中是非法的、高风险、高危害的网站地址列表，符合该库的访问会被禁止。

(5) 模块检查。防火墙能够控制是否允许某个模块访问网络。当应用程序访问网络的时候，对参与访问的模块进行检查，根据模块的访问规则决定是否允许该访问。以往的防火墙只是对应用程序进行检查，而没有对所关联的 dll 做检查。进行模块检查防止了木马模块注入到正常进程中访问网络。

6.2 天网防火墙实验

实验器材

- 天网防火墙个人版软件系统 1 套。
- PC(Windows XP/Windows 7)1 台。

预习要求

- 做好实验预习，复习防火墙技术的有关内容。
- 复习天网防火墙的使用方法。
- 熟悉实验过程和基本操作流程。
- 做好预习报告。

实验任务

通过本实验，掌握天网防火墙的安装及基本配置；学会利用天网防火墙保护系统安全。

实验环境

装有 Windows XP/Windows 7 操作系统的 PC。

预备知识

- 防火墙技术及原理。
- 网络协议。

实验步骤

1. 基本设置

如图 6.1 所示，系统设置有启动、规则设定、应用程序权限、局域网地址设定、其他设置几个方面。

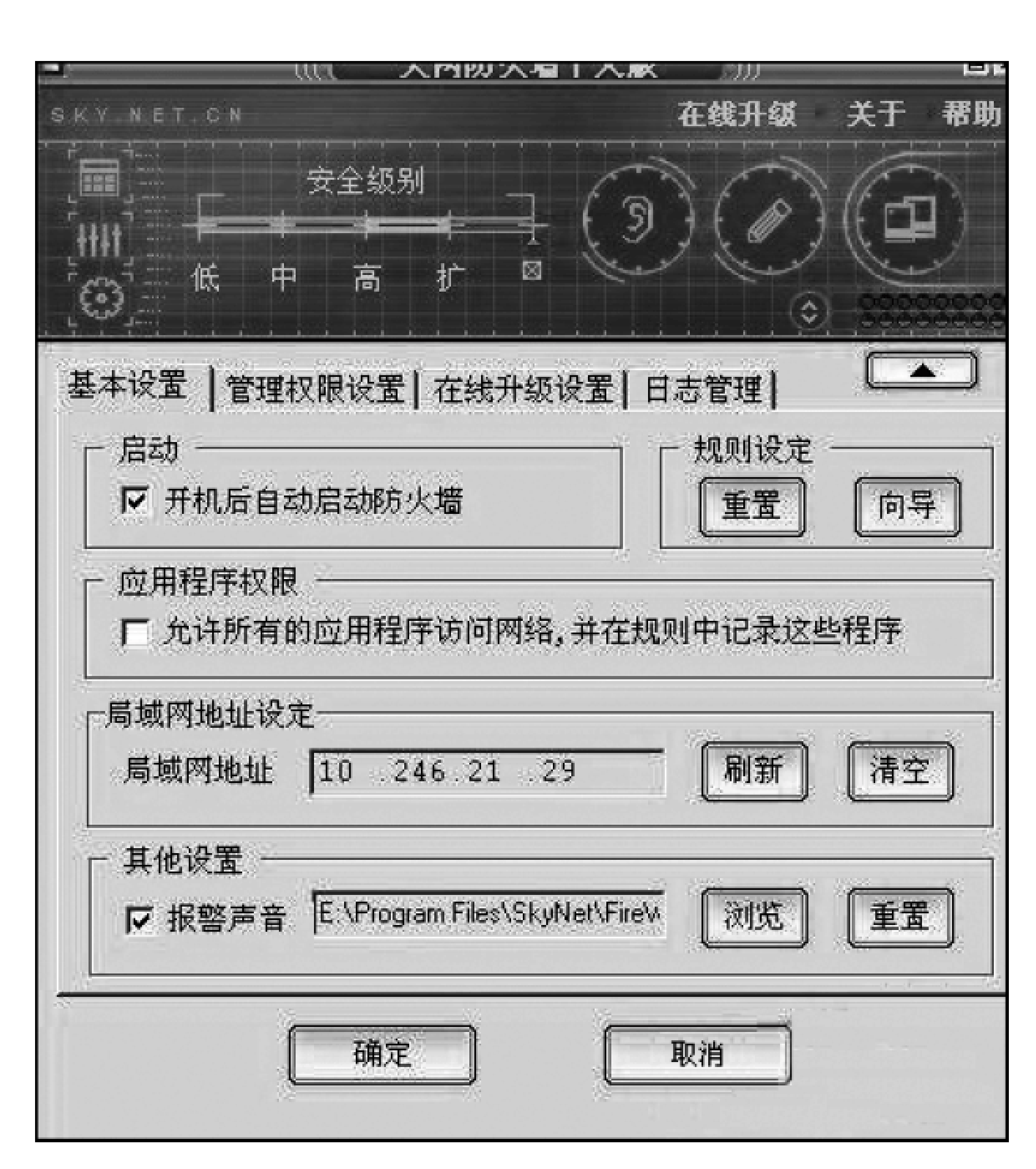


图 61　天网防火墙设置界面

"启动"项是设定开机后自动启动防火墙，在默认情况下不启动，一般选择自动启动。这也是安装防火墙的目的。"规则设定"是个设置向导，可以分别设置安全级别、局域网信息设置、常用应用程序设置。用户可以根据网络环境和爱好对"局域网地址设定"和"其他

设置"进行自由设置。

2. 安全级别设置

最新版的天网防火墙的安全级别分为高、中、低、自定义四类。把鼠标置于某个级别上时，可从注释对话框中查看详细说明，如图 6.2 所示。

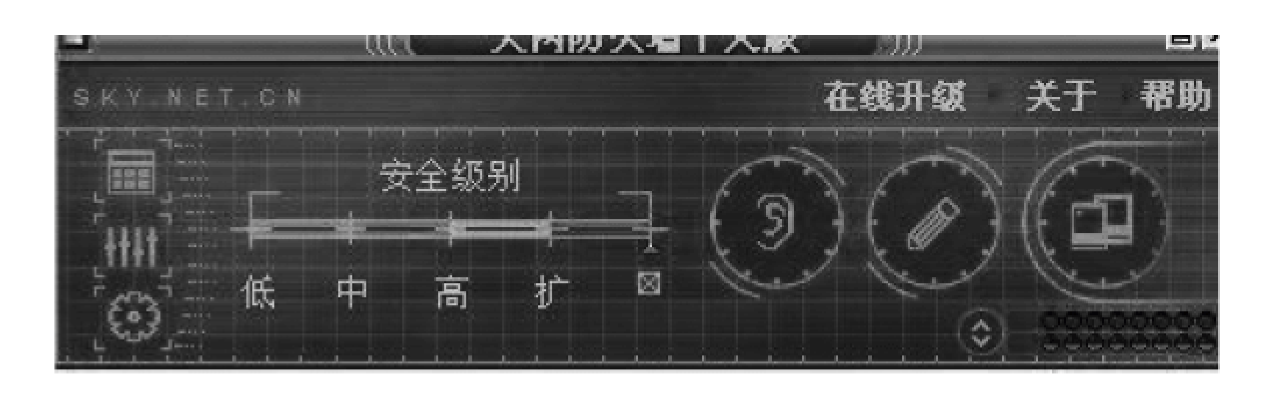


图 6.2　安全级别设置界面

- 低安全级别情况下，完全信任局域网，允许局域网中的机器访问自己提供的各种服务，但禁止互联网上的机器访问这些服务。
- 中安全级别下，局域网中的机器只可以访问共享服务，但不允许访问其他服务，也不允许互联网中的机器访问这些服务，同时运行动态规则管理。
- 高安全级别下，系统屏蔽掉所有向外的端口，局域网和互联网中的机器都不能访问自己提供的网络共享服务，网络中的任何机器都不能查找到该机器的存在。
- 自定义级别适合了解 TCP/IP 协议的用户，可以设置 IP 规则，而如果规则设置不正确，可能会导致不能访问网络。

对普通个人用户，一般推荐将安全级别设置为中级。

3. 应用程序访问网络权限设置

在设置的高级选项中，可以设置该应用程序是通过 TCP 还是 UDP 协议访问网络，及 TCP 协议可以访问的端口，当不符合条件时，程序将询问用户或禁止操作，如图 6.3 所示。

4. 自定义 IP 规则设置

在选中中级安全级别时，进行自定义 IP 规则的设置是很必要的。在这一项设置中，可以自行添加、编辑、删除 IP 规则，对防御入侵可以起到很好的效果，如图 6.4 所示。



图 6.3　应用程序访问网络权限设置



图 6.4　IP 访问规则设置

对于对 IP 规则不甚精通，并且也不想去了解这方面内容的用户，通过下载天网或其他网友提供的安全规则库，将其导入到程序中，也可以起到一定的防御木马程序、抵御入侵的效果，缺点是对于最新的木马和攻击方法，需要重新进行规则库的下载。

IP 规则的设置分为规则名称的设定，规则的说明，数据包方向，对方 IP 地址，对于该规则 IP、TCP、UDP、ICMP、IGMP 协议需要做出的设置，当满足上述条件时对数据包的处理方式，对数据包是否进行记录等。如果 IP 规则设置不当，天网防火墙的警告标志就会闪个不停；而如果正确地设置了 IP 规则，则既可以起到保护计算机安全的作用，又可以不必时时去关注警告信息。

用 Ping 命令探测计算机是否在线是黑客经常使用的方式，因此要防止别人用 Ping 探测。

在国内 IP 地址缺乏的情况下，很多用户是在局域网下上网，而在局域网内可能存在很多想一试身手的黑客。139 端口是经常被黑客利用 Windows 系统的 IPC 漏洞进行攻击的端口，用户可以对通过这个端口传输的数据进行监听或拦截，规则是名称可定为 139 端口监听，外来地址设为任何地址，在 TCP 协议的本地端口可填写从 139 到 139，通行方式可以是通行并记录，也可以是拦截，这样就可以对这个端口的 TCP 数据进行操作。445 端口的数据操作类似。

如果用户知道某个木马或病毒的工作端口，就可以通过设置 IP 规则封闭这个端口。方法是增加 IP 规则，在 TCP 或 UDP 协议中将本地端口设为从该端口到该端口，对符合该规则的数据进行拦截，就可以起到防范该木马的效果。

增加木马工作端口的数据拦截规则，是 IP 规则设置中最重要的一项技术。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

6.3 瑞星防火墙实验

实验器材

- 瑞星防火墙个人版软件系统 1 套。
- PC(Windows XP/Windows 7)1 台。

预习要求

- 做好实验预习，复习防火墙技术的有关内容。
- 复习瑞星防火墙的使用方法。
- 熟悉实验过程和基本操作流程。
- 做好预习报告。

实验任务

通过本实验，掌握瑞星防火墙的安装及基本配置；学会利用瑞星防火墙保护系统安全。

实验环境

装有 Windows XP/Windows 7 操作系统的 PC。

预备知识

- 防火墙技术及原理。
- 网络协议。

实验步骤

1. 启动瑞星个人防火墙软件

采用下列方法之一可以启动瑞星个人防火墙软件，启动后的界面如图 6.5 所示：

(1) 用鼠标双击桌面上的“瑞星个人防火墙”快捷图标。

(2) 单击“开始”按钮，选择“程序”|“瑞星个人防火墙”|“瑞星个人防火墙”。提示：一般情况下，瑞星个人防火墙在系统启动时将自动启动。



图 65　瑞星个人防火墙窗口

2. 设置安全级别

在防火墙程序窗口的右下角，拖动滑块到最右侧，即可设定安全级别为“高级”。提示：关于安全级别的定义及规则如下。

- 普通：系统在信任的网络中，除非规则禁止的，否则全部放过。
- 中级：系统在局域网中，默认允许共享，但是禁止一些较危险的端口。
- 高级：系统直接连接 Internet，除非规则放行，否则全部拦截。

3. 扫描木马病毒

选择防火墙程序窗口上的“操作”菜单，选择“扫描木马病毒”命令，将在屏幕右下角弹出扫描窗口，扫描结束后将给出提示，单击提示框中的“详细信息”按钮可以查看具体的扫描结果日志。

4. 黑、白名单的设置

1）黑名单的设置

黑名单用于设置禁止与本机通信的计算机列表，例如，可以把攻击本机的计算机加入此名单。选择“设置”菜单下的“详细设置”命令，打开“详细设置”对话框；单击“规则设置”下的“黑名单”；单击“增加规则”按钮，弹出一个如图 6.6 所示的“增加黑名单”对话框；在“地址类型”下拉列表框中选择“特定地址”或“地址范围”；在“输入地址”文本框中输入被禁止与本机通信的 IP 地址；单击“保存”按钮，即可完成设置。

增加黑名单
输入名称：
地址类型：特定地址
输入地址：0 . 0 . 0 . 0
保 存
取 消(C)

图 6.6 “增加黑名单”对话框

2）白名单的设置

白名单用于设置完全信任的计算机列表，列表中的计算机对本机有完全访问权限。具体操作参看黑名单的设置。

5. 修改应用程序访问网络的访问规则

(1) 选择“设置”菜单下的“详细设置”命令，打开“详细设置”对话框。

(2) 选择“规则设置”下的“访问规则”命令，打开如图 6.7 所示的对话框。



图 6.7 访问规则设置

(3) 允许或禁止应用程序访问网络。在程序列表框中选择一个应用程序，如“Telnet”；单击“编辑规则”按钮，弹出如图 6.8 所示的“编辑访问规则”对话框；在“常规”模式下选择“禁止”；单击“保存”按钮，即可禁止 Telnet 程序访问网络。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。



图 6.8 “编辑访问规则”对话框

- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

6.4 防火墙评测实验

实验器材

- 天网防火墙软件系统 1 套。
- 瑞星防火墙软件系统 1 套。
- 江民防火墙软件系统 1 套。
- PC(Windows XP/Windows 7)1 台。

预习要求

- 做好实验预习，复习防火墙技术的有关内容。
- 复习天网防火墙等多种防火墙的使用方法。
- 熟悉实验过程和基本操作流程。
- 做好预习报告。

实验任务

通过本实验，掌握主流防火墙的性能和功能。

实验环境

装有 Windows XP/Windows 7 操作系统的 PC。

预备知识

防火墙技术及原理。

实验步骤

(1) 完整记录天网防火墙、瑞星防火墙控制的实验内容。

（2）从 6.1.2 小节中选择江民防火墙或自行确定另外一种类型的软件防火墙，进行控制实验。

（3）确定防火墙的性能、功能、特定功能三个方面作为评测分析报告的主体。

（4）撰写并完成评测分析报告。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

第 7 章　入侵检测实验

随着计算机技术的发展，网络日趋复杂，传统防火墙的弱点和不足逐渐暴露出来，因此引发人们对入侵检测系统技术的研究和开发。网络入侵检测系统可以弥补防火墙的不足，为网络安全提供实时的入侵检测，并采取相应的防护手段。入侵检测技术是近 20 年来出现的一种主动保护自己免受黑客攻击的新型网络安全技术。从系统运行过程中产生的或系统所处理的各种数据中查找出威胁系统安全的因素，并对威胁做出相应的处理，就称为入侵检测。响应的软件或硬件称为入侵检测系统。入侵检测系统被称为是防火墙之后的第二道防门，它在不影响网络性能的情况下对网络进行检测，提供对内部攻击、外部攻击的实时保护。

7.1　入侵检测原理

7.1.1　入侵检测步骤

入侵检测一般分为两个步骤：信息收集和数据分析。

入侵检测利用的信息一般来自以下四个方面：系统日志、目录以及文件中的异常改变、程序执行中的异常行为和物理形式的入侵信息。

（1）系统日志：利用系统日志是检测入侵的必要条件。日志文件中记录了各种行为类型，每种类型又包含不同的信息，对用户活动来讲，不正常的或不期望的行为就是重复登录失败以及非授权访问重要文件等。

（2）目录以及文件异常：网络环境中的文件系统包含很多软件和数据文件，包含重要信息的文件和私有数据文件经常是被修改或破坏的目标。

（3）程序执行异常：网络系统上的程序执行一般包括操作系统、网络服务、用户启动的程序和应用。每个在系统上执行的程序由一到多个进程来实现。每个进程在具有不同权限的环境中执行，这种环境控制着进程可访问的系统资源、程序和数据文件等。

（4）物理形式的入侵信息：一是未授权的网络硬件连接；二是物理资源的未授权访问。

7.1.2　检测技术特点

在使用入侵检测技术时，应该注意具有以下技术特点的应用要根据具体情况进行选择。

1）信息收集分析时间

信息收集分析时间可分为固定时间间隔和实时收集分析两种。

采用固定时间间隔方法，在固定间隔的时间段内收集和分析这些信息。这种技术适

用于对安全性能要求较低的系统，对系统的开销影响较小；但这种技术的缺点是在时间间隔内将失去对网络的保护。

采用实时收集和分析技术可以实时地抑制攻击，使系统管理员及时了解并阻止攻击，系统管理员也可以记录黑客的信息；缺点是加大了系统开销。

2）采用的分析类型

采用的分析类型分为签名分析、统计分析和完整性分析。

签名分析就是同攻击数据库中的系统设置和用户行为模式匹配。在许多入侵检测系统中，都建有这种已知攻击的数据库。这种数据库可以经常更新，以对付新的威胁。签名分析的优点在于能够有针对性地收集系统数据，减少了系统的开销，如果数据库不是特别大，那么签名分析比统计分析更为有效。

统计分析用来发现偏离正常模式的行为，通过分析正常应用的属性得到系统的统计特征，对每种正常模式计算出均值和偏差，当侦测到有的数值偏离正常值时，就发出报警信号。这种技术可以发现未知的攻击，尤其是复杂的攻击，但统计传感器误码率较大。

完整性分析主要关注某些文件和对象的属性是否发生了变化。完整性分析通过被称为消息摘录算法的超强加密机制，可以感受到微小的变化。这种分析可以侦测到任何使文件发生变化的攻击，弥补了签名分析和统计分析的缺陷，但是这种分析的实时性很差。

3）对攻击和误用的反应

有些基于网络的检测系统可以针对侦测到的问题作出反应。这些反应主要有改变环境、效用检验、实时通知等。改变环境通常包括关闭连接、重新设置系统。由于改变了系统的环境，因此可以通过设置代理和审计机制获得更多的信息，从而跟踪黑客。许多实时系统还允许管理员选择一种预警机制，把发生的问题实时地送往各个地方。

4）管理和安装

用户采用检测系统时，需要根据本网的一些具体情况确定。实际上，没有两种完全相同的网络环境，因此，就必须对采用的系统进行配置。比如，可以配置系统的网络地址、安全条目等。某些基于主机的检测系统还提供友好的用户界面，让用户说明需要传感器采集哪些信息。

7.1.3 Snort 简介

Snort 是 Martin Roesch 等人开发的一种由 C 语言编写的开放源码的入侵检测系统。Martin Roesch 把 Snort 定位为一个轻量级的、跨平台、支持多操作系统的入侵检测系统。它具有实时数据流量分析和 IP 数据包日志分析的能力，具有跨平台特征，能够进行协议分析和对内容的搜索/匹配。它能够检测不同的攻击行为，如缓冲区溢出、端口扫描、DoS 攻击等，并进行实时报警。Snort 可安装在网络上的一台主机上对整个网络进行监视。

Snort 由三个子系统构成：数据包解码器、检测引擎、日志与报警系统。在使用 Snort 之前，需要根据网络环境和安全策略对 Snort 进行配置，主要包括设置网络变量、配置预处理器（preprocessors）、配置输出插件、配置所使用的规则集。在入侵检测过程中采用了规则匹配的检测方法，所以误报率较低。

Snort 有三种工作模式：嗅探器、数据包记录器、网络入侵检测系统。嗅探器模式仅仅是从网络上读取数据包并作为连续不断的流显示在终端上。数据包记录器模式把数据包记录到硬盘上。网络入侵检测模式是最复杂的，而且是可配置的，可以让 Snort 分析网络数据流以匹配用户定义的一些规则，并根据检测结果采取一定的动作。

7.1.3.1 功能特征

虽然 Snort 是一个轻量级的入侵检测系统，但是它的功能却非常强大，其特点如下：

(1) 跨平台性。可以支持 Linux、Solaris、UNIX、Windows 系列等平台，而大多数商用入侵检测软件只能支持一两种操作系统，甚至需要特定的操作系统。

(2) 功能完备。具有实时流量分析的能力，能够快速地监测网络攻击，并能及时地发出警报。使用协议分析和内容匹配的方式，提供了对 TCP、UDP、ICMP 等协议的支持，对缓冲区溢出、隐蔽端口扫描、CGI 扫描、SMB 探测、操作系统指纹特征扫描等攻击都可以检测。

(3) 使用插件的形式。方便管理员根据需要调用各种插件模块，包括输入插件和输出插件。

输入插件主要负责对各种数据包的处理，具备传输层连接恢复、应用层数据提取、基于统计的数据包异常检测的功能，从而拥有很强的系统防护功能，如使用 TCP 流插件，可以对 TCP 包进行重组。

输出插件则主要用来将检测到的报警以多种方式输出，通过输出插件可以输出到 MySQL、SQL 等数据库中，还可以以 XML 格式输出，也可以把网络数据保存到 TCPDump 格式的文件中；按照其输出插件规范，用户甚至可以自己编写插件，自己来处理报警的方式并进而作出响应，从而使 Snort 具有非常好的可扩展性和灵活性。

(4) Snort 规则描述简单。Snort 基于规则的检测机制十分简单和灵活，使得可以迅速对新的入侵行为做出反应，发现网络中潜在的安全漏洞。同时该网站提供几乎与 http://www.cert.org(应急响应中心，负责全球的网络安全事件以及漏洞的发布)同步的规则库更新，因此，甚至许多商业的入侵检测软件可以直接使用 Snort 的规则库。图 7.1 显示了 Snort 的系统组成和数据处理流程。

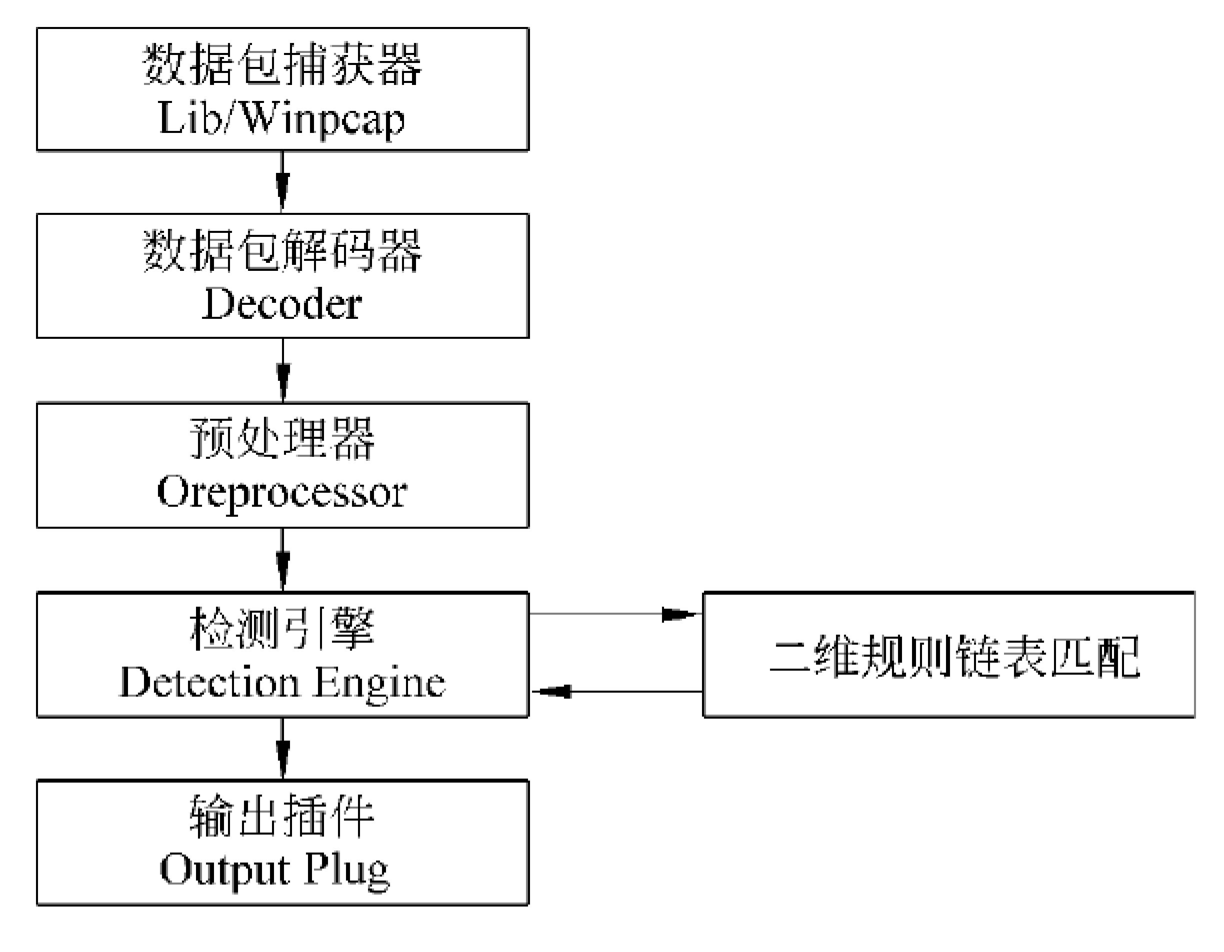


图 7.1 Snort 程序流程图

① 数据包捕获器。基于网络的入侵检测系统需要捕获并分析所有传输到监控网卡的网络数据，这就需要包捕获技术。Snort 通过两种机制来实现包捕获技术：一种是将网卡设置为混杂模式；另一种是利用 Libpcap/Winpcap 函数库从网卡捕获网络数据包。

数据包捕获函数库是一个独立的软件工具，能直接从网卡获取数据包。该函数库是由 Berkeley 大学 Lawrence Berkeley National Laboratory 研究院开发，Libpcap 支持所有基于可移植操作系统接口（portable operating system interface of UNIX，POSIX）的操作系统，如 Linux、UNIX 等，后来为支持跨平台特性，又开发了 Windows 版本（http://www. winpca p. org），Windows 下和 Linux 的函数调用几乎完全相同，Snort 就是通过调用该库函数从网络设备上捕获数据包。

② 数据包解码器。数据包解码器主要是对各种协议栈上的数据包进行解析、预处理，以便提交给检测引擎进行规则匹配。解码器运行在各种协议栈之上，从数据链路层到传输层，最后到应用层，因为当前网络中的数据流速度很快，如何保障较高的速度是解码器子系统中的一个重点。目前，Snort 解码器所支持的协议包括 Ethernet、SLIP 和 PPP 等。

③ 预处理器。预处理模块的作用是对当前截获的数据包进行预先处理，以便后续处理模块对数据包的处理操作。由于最大数据传输单元（MTU）限制及网络延迟等问题，路由器会对数据包进行分片处理。但是恶意攻击者也会故意发送经过软件加工过的数据包，以便把一个带有攻击性的数据包分散到各个小的数据包中，并有可能打乱数据包传输次序，分多次传输到目标主机。因此，对异常数据包的处理也是入侵检测系统的重要内容。

预处理器包括以下插件：

- 模拟 TCP/IP 堆栈功能的插件，如 IP 碎片重组、TCP 流重组插件。
- 各种解码插件，如 HTTP 解码插件、Unicode 解码插件、RPC 解码插件、Telnet 解码插件等。
- 规则匹配无法进行攻击检测时所用的插件，如端口扫描插件、Spade 异常入侵检测插件、Bo 检测插件、ARP 欺骗检测插件等。根据各预处理插件文件名可对此插件功能做出推断。

④ 检测引擎。检测引擎是入侵检测系统的核心内容，Snort 用一个二维链表存储它的检测规则，其中一维称为规则头，另一维称为规则选项。规则头中放置的是一些公共属性特征，而规则选项中放置的是一些入侵特征。Snort 从配置文件读取规则文件的位置，并从规则文件读取规则，存储到二维链表中。

Snort 的检测就是二维规则链表和网络数据匹配的过程，一旦匹配成功则把检测结果输出到输出插件。为了提高检测速度，通常把最常用的源/目的 IP 地址和端口信息放在规则头链表中，而把一些独特的检测标志放在规则选项链表中。规则匹配查找采用递归的方法进行，检测机制只针对当前已经建立的链表选项进行检测，当数据包满足一个规则时，就会触发相应的操作。Snort 的检测机制非常灵活，用户可以根据自己的需要很方便地在规则链表中添加所需要的规则模块。

(5) 日志和报警子系统。日志和报警子系统可以在运行 Snort 的时候以命令行交互

的方式进行选择，如果在运行时指定了命令行的输出开关，在 Snort 规则文件中指定的输出插件会被替代。现在可供选择的日志形式有三种，报警形式有六种。Snort 可以把数据包以解码后的文本形式或者 TCPDump 的二进制形式进行记录。解码后的格式便于系统对数据进行分析，而 TCPDump 格式可以保证很快地完成磁盘记录功能，第三种日志机制就是关闭日志服务，什么也不做。使用数据库输出插件，Snort 可以把日志记入数据库，当前支持的数据库包括 Postgresql、MySQL、Oracle 以及 UNIX ODBC 数据库。

7.1.3.2 基本操作

1. 启动

Snort 作为网络入侵检测系统，使用下面命令行可以启动这种模式：

```
Snort - dev - l log - h 192.168.1.0/24 - c Snort.conf
```

Snort 就会对每个包和规则集进行匹配，发现这样的包就会根据规则的设置采取相应的行动。如果不指定输出目录，Snort 就输出到/var/log/Snort 目录中。

也可以采用如下简单的命令方式：

```
Snort - i 2 - c Snort.conf
```

其中，i 选项为选择网卡；网络监控方式以及输出方式都在 Snort. conf 中被定义。

2. 输出

在网络入侵检测模式下，有多种方式来配置 Snort 的输出。在默认情况下，Snort 以 ASCII 格式记录日志，使用 full 报警机制。

Snort 有六种报警机制：full、fast、socket、syslog、smb（winpopup）和 none。其中，有四个可以在命令行状态下使用-A 选项设置。

- -A fast：报警信息包括一个时间戳（timestamp）、报警消息、源/目的 IP 地址和端口。
- -A full：是默认的报警模式。
- -A unsock：使 Snort 将报警信息通过 UNIX 的套接字发往一个负责处理报警信息的主机，在该主机上有一个程序在套接字上进行监听。
- -A none：关闭报警机制。

3. 规则集

规则集是 Snort 的攻击特征库，每条规则是一条攻击标识，Snort 通过它来识别攻击行为。Snort 使用一种简单的、轻量级的规则描述语言，这种语言灵活而强大。一条 Snort 规则可以从逻辑上分为两个部分：规则头（括号左边的内容）和规则选项（括号内的内容）。

规则头包含有匹配的行为动作、协议类型、源 IP 及端口、数据包方向、目标 IP 及端口。动作包括三类：告警（Alert）、日志（Log）和通行（Pass），表明 Snort 对包的三种处理方式。其中最常用的就是 Alert 动作，它会向报警日志中写入报警信息。

在源地址、目的地址、端口中可以使用 any 来代表任意的地址或端口，还可以使用符号“!”来表明取非运算。IP 地址可以被指定为一个 CIDR 的地址块，端口也可以指定一

个范围，在目的地址和源地址之间可以使用标识符“<-”和“->”来指明方向。

规则的选项部分是由一个或几个选项组合而成，选项之间用“;”分隔，选项关键字和值之间使用“:”分隔。对规则选项的分析构成了 Snort 检测引擎的核心。选项主要分为四类：数据包相关各种特征的说明选项、与规则本身相关的一些说明选项、规则匹配后的动作选项、对某些选项的进一步修饰。

下面是一个规则范例：

```
alert tcp any any->192.168.1.0/24 111(content:"|00 01 86 a5|"; msg: "mountd access";)
```

该规则表示监控的网络数据的协议为 TCP 协议，源地址、源端口为任意值，方向为由外向内，内部的网络地址为子网 192.168.1.0/24，端口号为 111，当发现数据包中有“00 01 86 a5”内容时，Snort 会发送报警信息 mountd access。

7.2 Snort 入侵检测实例

实验器材

- Snort 软件系统 1 套。
- PC(Windows XP/Windows 7)1 台。

预习要求

- 做好实验预习，复习入侵检测技术的有关内容。
- 熟悉 Snort 软件的使用方法。
- 熟悉实验过程和基本操作流程。
- 做好预习报告。

实验任务

通过本实验，掌握安装并运行一个 Snort 系统的方法；了解入侵检测系统的作用和功能。

实验环境

装有 Windows XP/Windows 7 操作系统的 PC 一台。

预备知识

入侵检测原理。

实验步骤

现将本实验需要的组件以及其作用和功能介绍如下。

(1) Winpcap：Windows 环境下的捕获网络数据包驱动程序库，下载地址：http://www.winpcap.org/。

(2) Snort：入侵检测主程序，网站提供 Windows 下的安装版本，可以直接下载安装。源代码在 Linux 下可以直接编译生成；在 Windows 下使用 Visual Studio 系列的编译器，在工程设置中将几个预处理设置禁止，可以编译通过，同时需要下载 Snort 规则。下载地址：http://www.snort.org/。

(3) Apache：为系统提供了 Web 服务支持，下载地址：http://www.apache.org/。

(4) PHP：为系统提供了 PHP 支持，使 Apache 能够运行 PHP 程序，下载地址：http://www.php.net/。

(5) MySQL：存储各种报警事件的数据库系统，下载地址：http://www.mysql.com/。

(6) ACID：ACID(analysis console for intrusion databases)是基于 PHP 的入侵检测数据库分析控制台，它能够处理由各种入侵检测系统、防火墙等安全工具产生并放入数据库中的安全事件，安装 PHP 就是为了使用 ACID，下载地址：http://acidl ab.sourceforge.net/。

(7) Adodb：Adodb 是 PHP 连接数据库的组件，下载地址：http://adodb.sourceforge.net/。

(8) Jpgraph：由 PHP 编写的基于面向对象技术的图形显示链接库，ACID 通过 Adodb 读取 Snort 在 MySQL 中产生的数据，将分析结果显示在网页上，并使用 Jpgraph 组件对其进行图形化显示分析。下载地址：http://www.aditus.nu/jpgraph/。

1. 安装 Apache 服务器

(1) 双击 httpd-2.2.17-win32-x86-no_ssl.msi。

(2) 出现 Windows 标准的软件安装欢迎界面，直接单击 Next 按钮继续，出现授权协议，选择同意授权协议，然后继续，出现安装说明。

(3) 在 Network Domain 中填写网络域名，如 kysf.net ，如果没有网络域名，可以任意填写。如果架设的 Apache 服务器要放入 Internet ，则一定要填写正确的网络域名。在 Server Name 中填入服务器名，如 www.kysf.net，即主机名。在 Administrator's Email Address 中填写系统管理员的电子邮件地址，如 indian@163.com。上述三条信息仅供参考，其中，电子邮件地址会在系统出现故障时提供给访问者，如图 7.2 所示。

图 7.2 Apache 安装界面

(4) 确认安装选项无误，如果要再检查一遍，可以单击 Back 按钮返回检查。单击 Install 按钮开始安装。

(5) 检测方法：若选择端口 8080，使用“httpd -k install.”命令将 Apache 设置为 Windows 中的服务(如果是 Apache 2.2 之前的版本，输入“apache -k install”)，如图 7.3 所示；若选择端口 80，则无需进行该步骤。

```
:\Apache2.2\bin>cd c:\

:\>cd apache2.2\bin

:\Apache2.2\bin>httpd -k install
nstalling the Apache2.2 service
he Apache2.2 service is successfully installed.
esting httpd.conf....
rrors reported here must be corrected before the service can be started.
ttpd: Could not reliably determine the server's fully qualified domain name, us
ing 192.168.1.233 for ServerName

:\Apache2.2\bin>
```

图 7.3 8080端口检测界面

(6) 通过上述方式，在 DOS 或者浏览器下运行，均有启动成功显示。

选择定制安装，安装在默认文件夹 C:\apache 下。安装程序会在该文件夹下自动产生一个子文件夹 apache2，继续完成安装。如图 7.4 所示，打开配置文件 C:\Apache\apache2\conf\httpd.conf(版本不同，可能是 C:\Apache\conf\httpd.conf)，将其中的 Listen 8080 更改为 Listen 50080。这是由于 Windows IIS 中的 Web 服务器默认情况下在 TCP 80 端口监听连接请求，而 8080 端口一般留给代理服务器使用，所以为了避免 Apache Web 服务器的监听端口与其发生冲突，将 Apache Web 服务器的监听端口修改为不常用的高端端口 50080。如果安装的时候 80 端口未被占用，则无需修改端口。

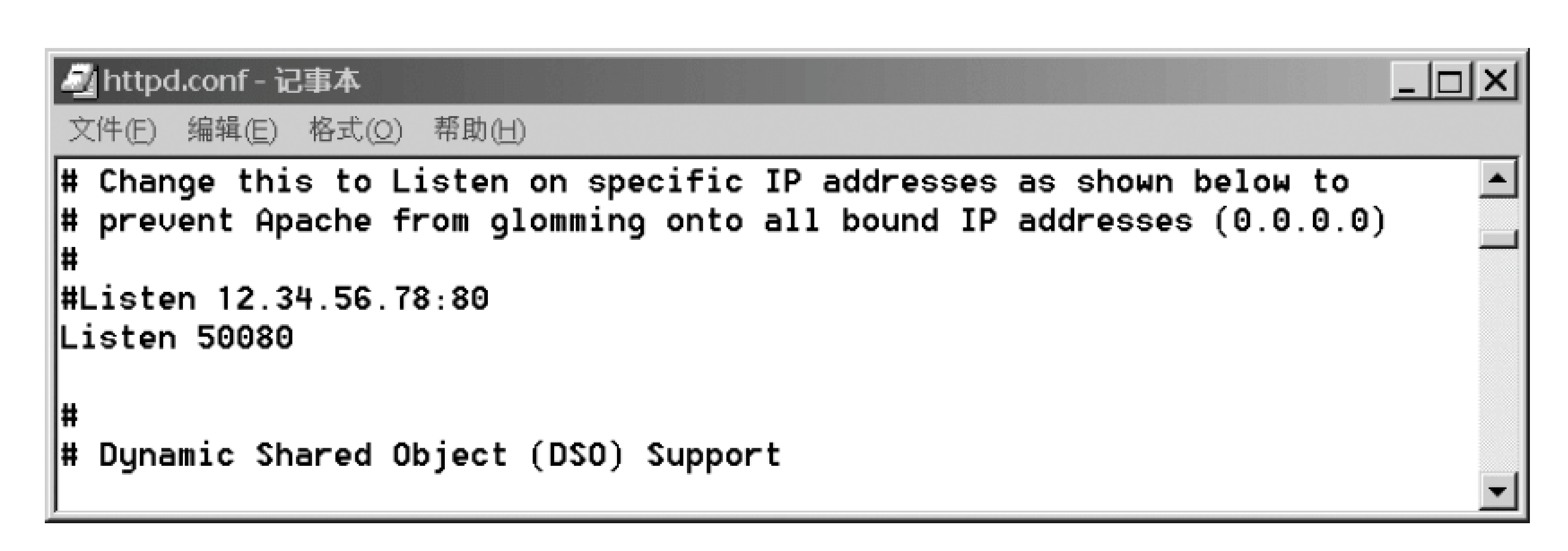


图 7.4 Apache配置界面

选择“开始”|“运行”命令，输入“cmd”，进入命令行方式。输入下面的命令：

```
C:\> cd apache\apache2\bin
C:\apache\apache2\bin\apache - k install
```

这是将 Apache 设置为 Windows 中的服务方式运行。

在浏览器中进行访问时，使用 http://localhost:50080/即可。

2. 添加 Apache 对 PHP 的支持

(1) 解压缩 php-5.2.6-Win32.zip 至 C:\Php。

(2) 将 php5ts.dll 文件复制到%systemroot%\system32。

(3) 将 php.ini-dist (修改文件名)复制到%systemroot%\php.ini，修改 php.ini：

```
extension=php_gd2.dll
extension=php_mysql.dll
```

如果 php.ini 有该句，将此语句前面的“;”注释符去掉，如图 7.5 所示。

```
php.ini - 记事本
文件(F)  编辑(E)  格式(O)  帮助(H)
;extension=php_domxml.dll
;extension=php_exif.dll
;extension=php_fdf.dll
;extension=php_filepro.dll
extension=php_gd2.dll
;extension=php_gettext.dll
;extension=php_hyperwave.dll
;extension=php_iconv.dll
```

图 7.5　PHP 配置界面

同时复制 C:\Php\extension 下的 php_gd2.dll 和 php_mysql.dll 至%systemroot%\。

(4) 添加 gd 图形库的支持，在 C:\Apache\Apache2\conf\httpd.conf 中添加：

```
LoadModule php5_module "C:/Php5/php5apache2.dll"
```

注意：Apache 版本在 2.2 以上的要换成 LoadModule php5_module "C:/Php5/php5apache2_2.dll"，否则无法 restart。

在 AddType application 一行下面加入两行信息：

```
AddType application/x-httpd-php .php .phtml .php3 .php4
AddType application/x-httpd-php-source .phps
```

(5) 添加好后，保存 http.conf 文件。单击“开始”按钮，选择“运行”命令，在弹出的窗口中输入 cmd 进入命令行方式，输入命令：net start apache2，在 Windows 中启动 Apache Web 服务，如图 7.6 所示。



图 7.6　Apache 启动界面

测试 PHP 脚本：

在 C:\Apache2\htdocs 目录下新建 test.php，test.php 文件内容：

```
<?phpinfo();?>
```

使用 http://localhost/test.php(或 http://127.0.0.1:50080/test.php)测试 PHP 是否安装成功。

3. 安装配置 Snort

安装程序 WinPcap_4_0_2.exe,默认安装即可。

版本一:安装 Snort_2_8_1_Installer.exe,默认安装即可,Snort 的默认安装路径为 C:\Snort。

将 snortrules-snapshot-CURRENT 目录下的所有文件复制(全选)到 C:\Snort 目录下。

将文件压缩包中的 snort.conf 覆盖 C:\Snort\etc\snort.conf。

版本二:安装 Snort_2_9_0_1_Installer.exe,默认安装即可,Snort 的默认安装路径为 C:\Snort。

将 snortrules-snapshot-CURRENT 目录下的所有文件复制(全选)到 C:\Snort\rules 目录下。

文件 open-test.conf 中会有 snortrules 的规则,对应 C:\Snort\etc 下的 snort.conf 内部的使用规则,可以自行更改。

4. 安装 MySQL 配置 MySQL

(1) 解压 mysql-5.0.51b-win32.zip,并安装到默认文件夹 C:\Mysql。采取默认安装。设置数据库实例流程,如图 7.7 至图 7.14 所示。

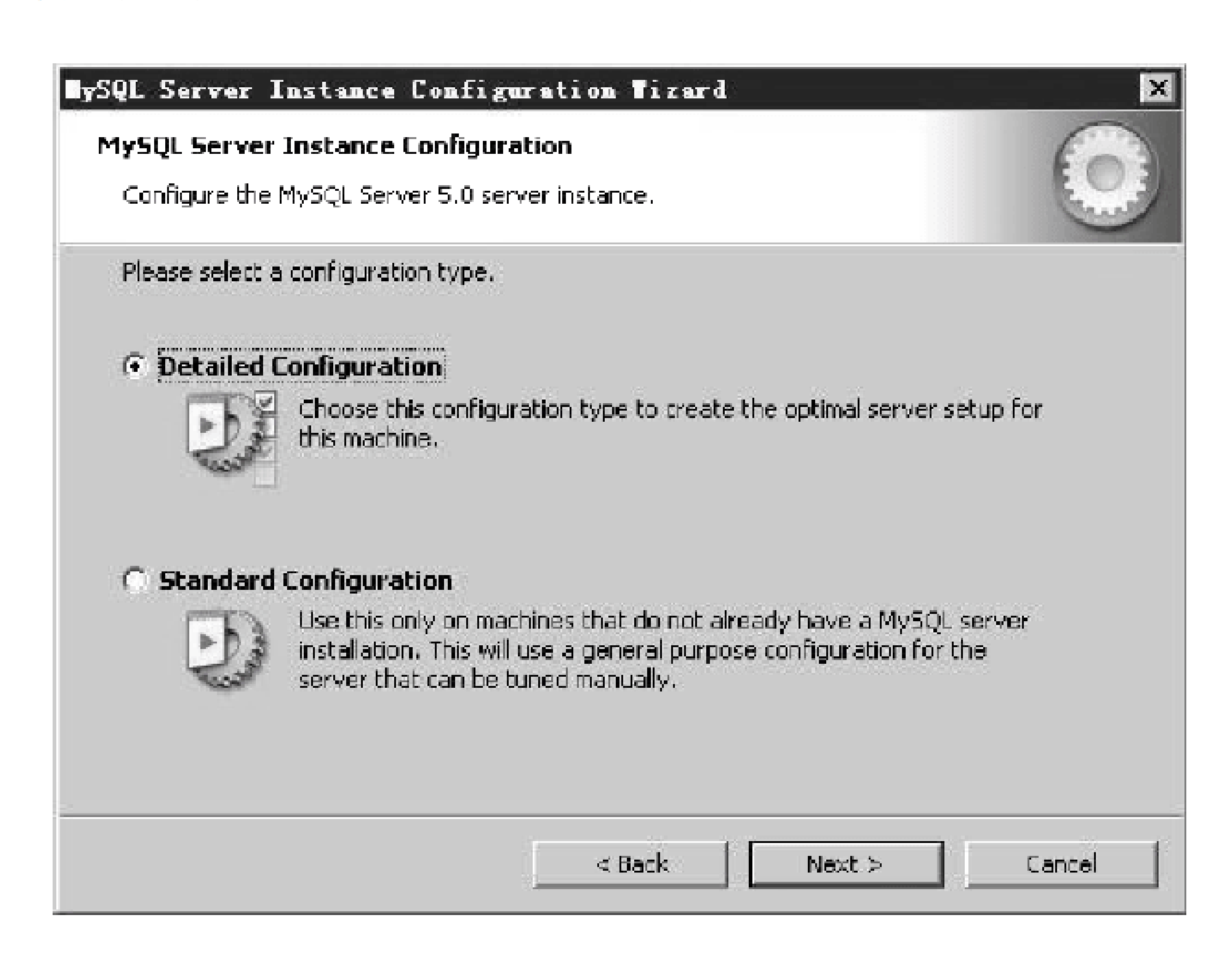


图 7.7 MySQL 安装向导界面-1

安装路径:C:\Program Files\MySQL\MySQL Server 5.1。

(2) 在命令行方式下输入 net start mysql,启动 MySQL 服务,显示"请求的服务已经启动"。

(3) 注意设置 root 账号和密码,并在命令行方式下进入 C:\Mysql\bin,输入下面的命令:

```
C:\Mysql\bin\mysqld - nt - install
```



图 7.8　MySQL 安装向导界面-2

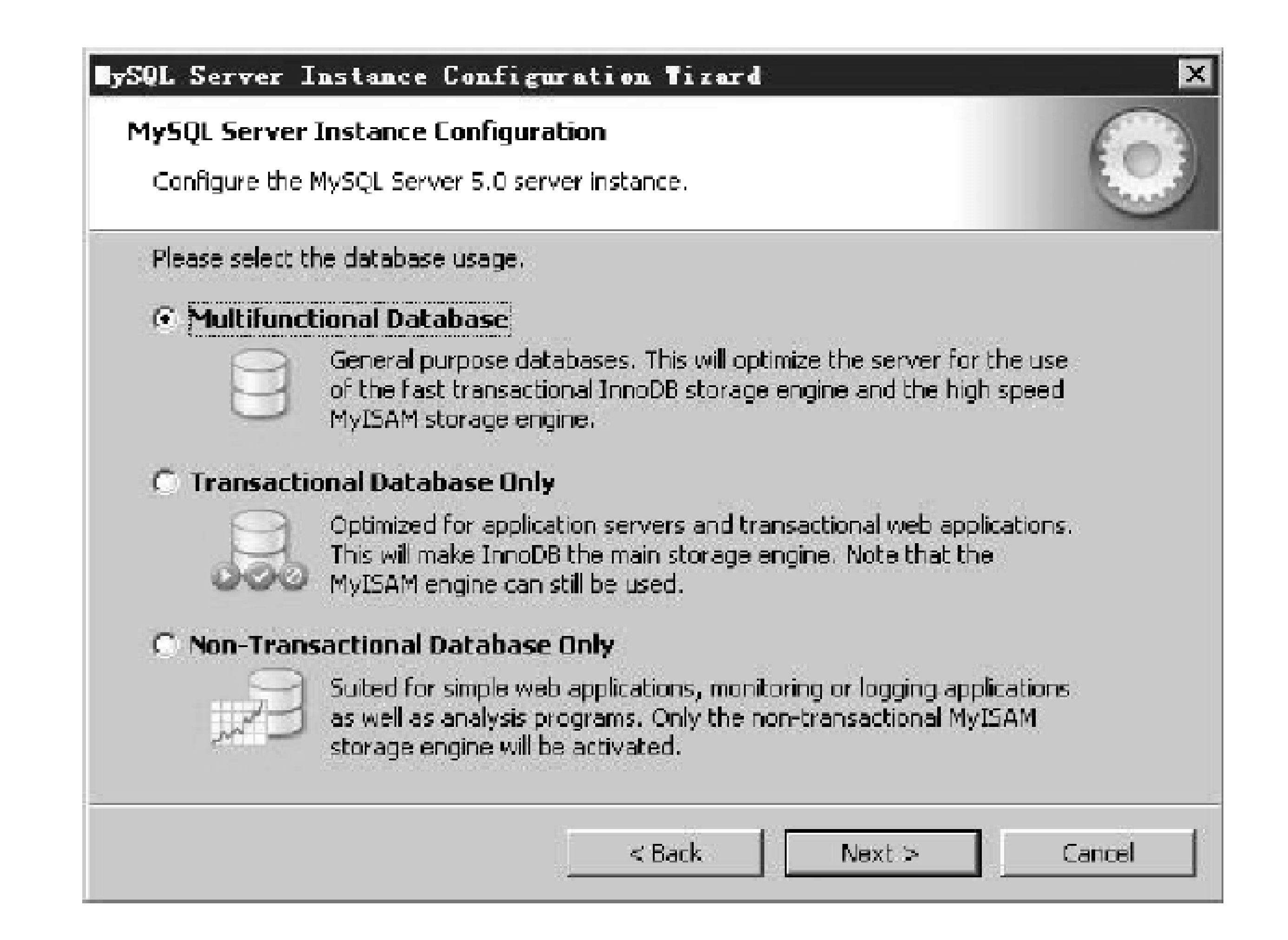


图 7.9　MySQL 安装向导界面-3

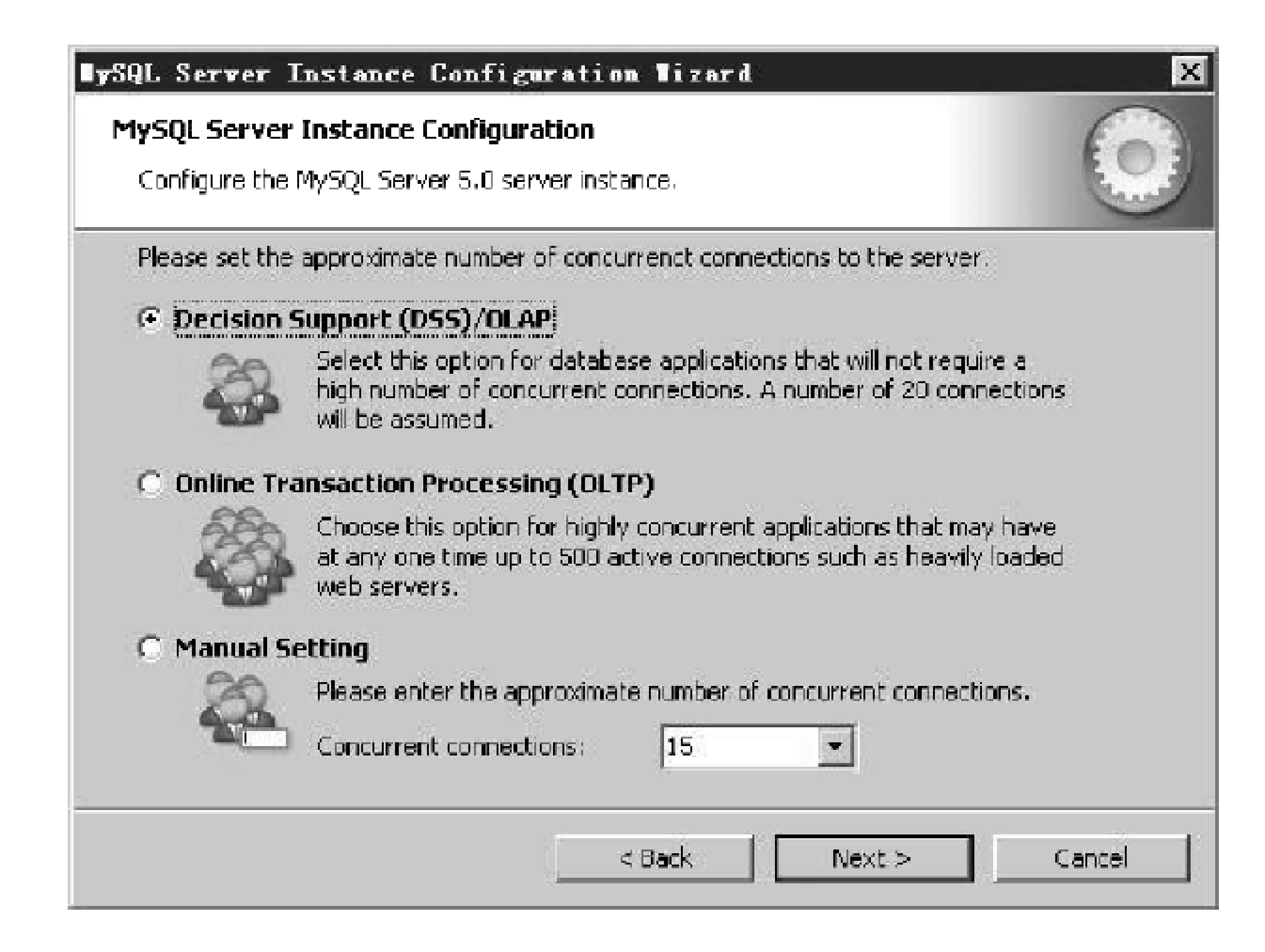


图 7.10　MySQL 安装向导界面-4

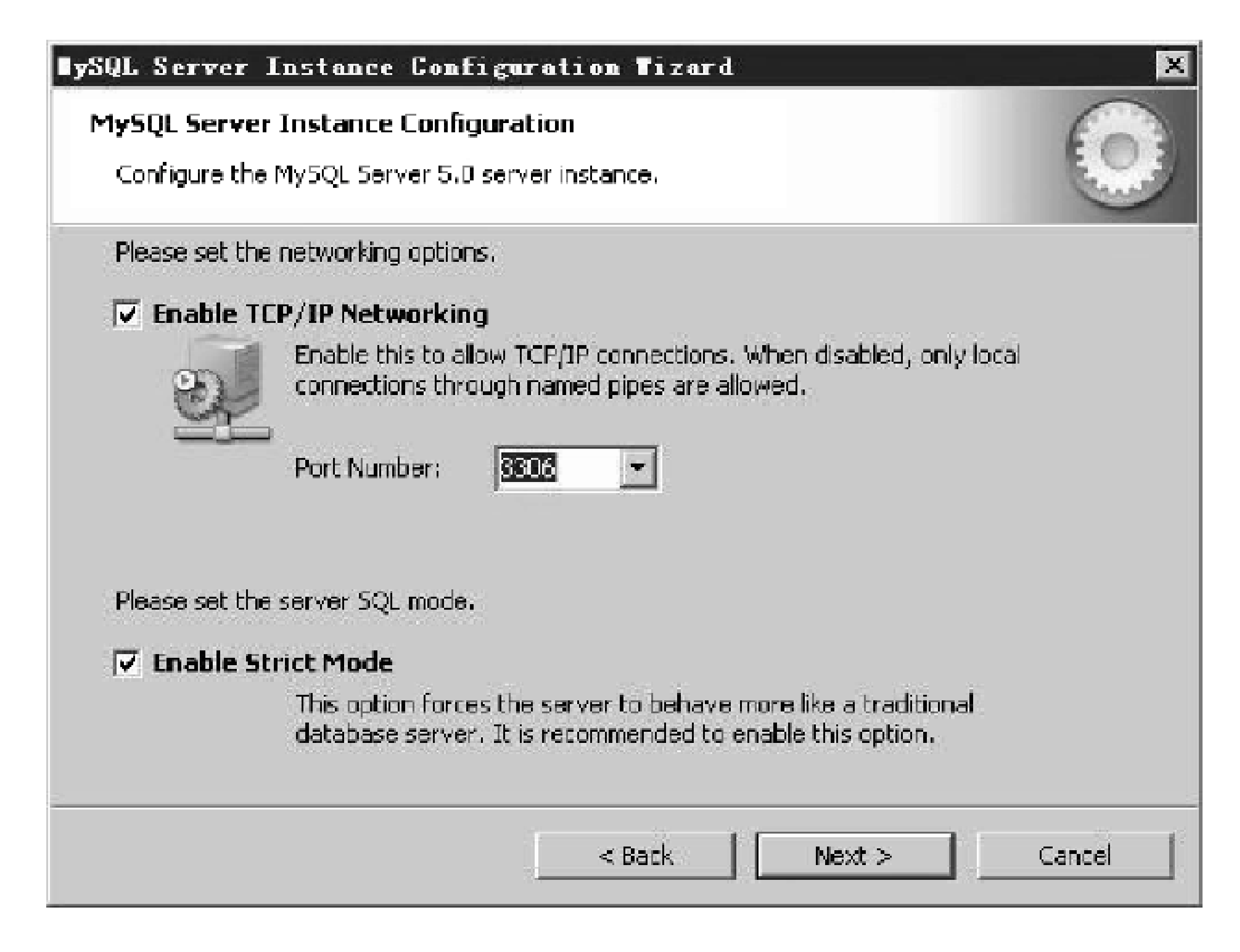


图 7.11　MySQL 安装向导界面-5

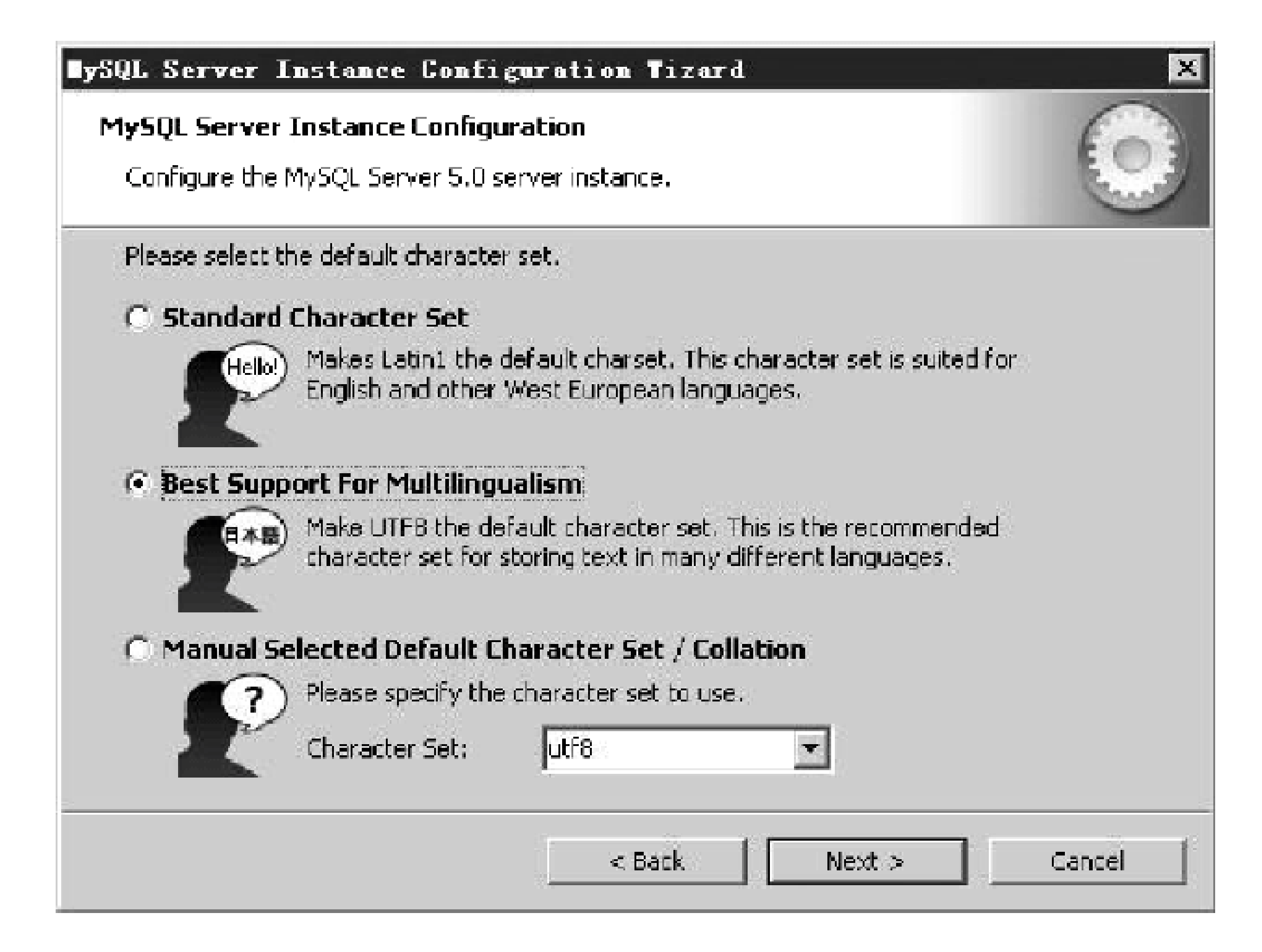


图 7.12　MySQL 安装向导界面-6

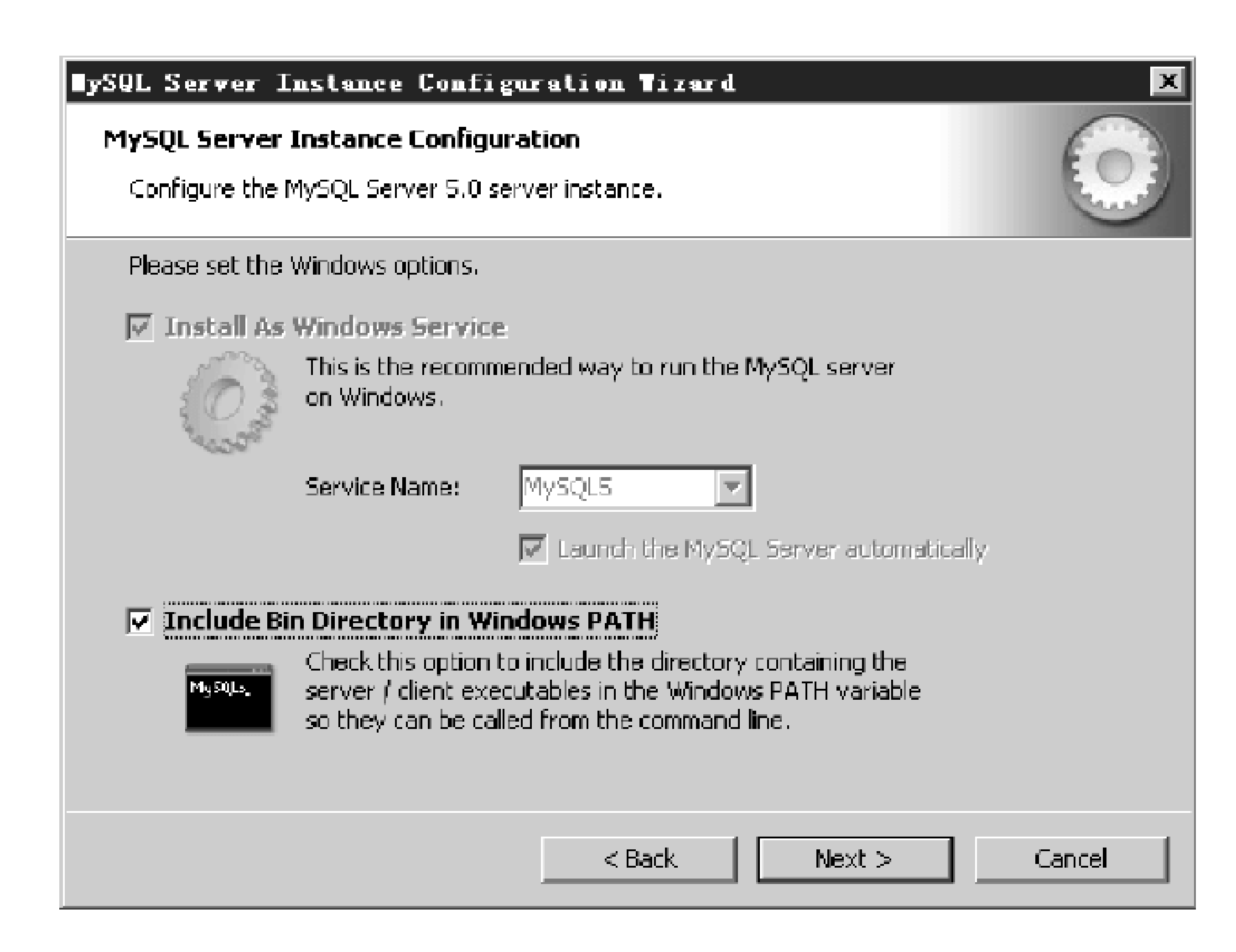


图 7.13　MySQL 安装向导界面-7

图 7.14　MySQL 安装向导界面-8

在命令行方式下输入 net start mysql，启动 MySQL 服务。在安装目录下（一般为 C:\Mysql\bin）单击“开始”按钮，选择“运行”命令，输入命令：cmd，在出现的命令行窗口中输入下面的命令：

```
C:\> cd mysql\bin
C:\Mysql\bin> mysql -u root -p
```

输入刚才设置的 root 密码，运行以下命令：

```
create database Snort;                    //在输入分号后 MySQL 才会编译执行语句
create database Snort_archive;
                    //create 语句建立了 Snort 运行必需的 Snort 数据库和 snort_archive 数据库
```

运行以下命令：

```
C:\Mysql\bin\mysql -D snort -u root -p< C:\Snort\contrib\create_mysql
C:\Mysql\bin\mysql -D snort_archive -u root -p< C:\Snort\contrib\create_mysql
```

上面两个语句表示以 root 用户身份使用 C:\Snort\contrib 目录下的 create_mysql 脚本文件，在 Snort 数据库和 Snort_archive 数据库中建立了 Snort 运行必需的数据表。再次以 root 用户登录 MySQL 数据库，在提示符后输入下面的语句：

```
grant usage on * .* to "acid"@ "localhost" identified by "acidtest";
grant usage on * .* to "Snort"@ "localhost" identified by "Snorttest";
```

上面两个语句表示在本地数据库中建立了 acid（密码为 acidtest）和 Snort（密码为 Snorttest）两个用户，以备后面使用。

```
set password for "acid"@ "localhost"=password('123');
set password for "Snort"@ "localhost"=password('123');
grant select,insert,update,delete,create,alter on Snort .* to "acid"@ "localhost";
grant select,insert,update,delete,create,alter on Snort_archive .* to "acid"@ "localhost";
grant select,insert,update,delete,create,alter on Snort .* to "Snort"@ "localhost";
```

```
grant select,insert,update,delete,create,alter on Snort_archive .* to "snort"@"localhost";
```

上述操作是为新建的用户在 Snort 和 Snort_archive 数据库中分配权限。

建立 Snort 输出安全事件所需要的表，其中 C:\Snort 为 Snort 的安装目录。

5. 安装其他工具

(1) 安装 Adodb，解压缩 adodb497.zip 到 C:\Php\adodb 目录下。

(2) 安装 Jpgrapg 库，解压缩 jpgraph-1.22.1.tar.gz 到 C:\Php\jpgraph，并且修改 C:\Php\jpgraph\src\jpgraph.php，添加如下一行：

```
DEFINE("CACHE_DIR","/tmp/jpgraph_cache/");
```

(3) 安装 ACID，解压缩 acid-0.9.6b23.tar.gz 到 C:\Apache\htdocs\acid 目录下，并将 C:\Apache\htdocs\acid\acid_conf.php 文件的如下各行内容修改为：

```
$DBlib_path="C:\Php\adodb";
$DBtype="mysql";
$alert_dbname="snort";
$alert_host="localhost";
$alert_port="3306";
$alert_user="acid";
$alert_password="acid";
/* Archive DB connection parameters */
$archive_dbname="snort_archive";
$archive_host="localhost";
$archive_port="3306";
$archive_user="acid";
$archive_password="acid";
$ChartLib_path="C:\Php\jpgraph\src";
```

(4) 通过浏览器访问 http:/127.0.0.1/acid/acid_db_setup.php，在打开的页面中单击 Create ACID AG 按钮，让系统自动在 MySQL 中建立 ACID 运行必需的数据库，如图 7.15 所示。

6. 启动 Snort

打开 C:\Snort\etc\snort.conf 文件，将文件中的下列语句

```
include classification.config
include reference.config
```

修改为绝对路径：

```
include C:\Snort\etc\classification.config
include C:\Snort\etc\reference.config
```

在该文件的最后加入以下语句：

```
output database: alert, mysql, host=localhost user=snort password=snorttest dbname=snort encoding=
hex detail=full
```

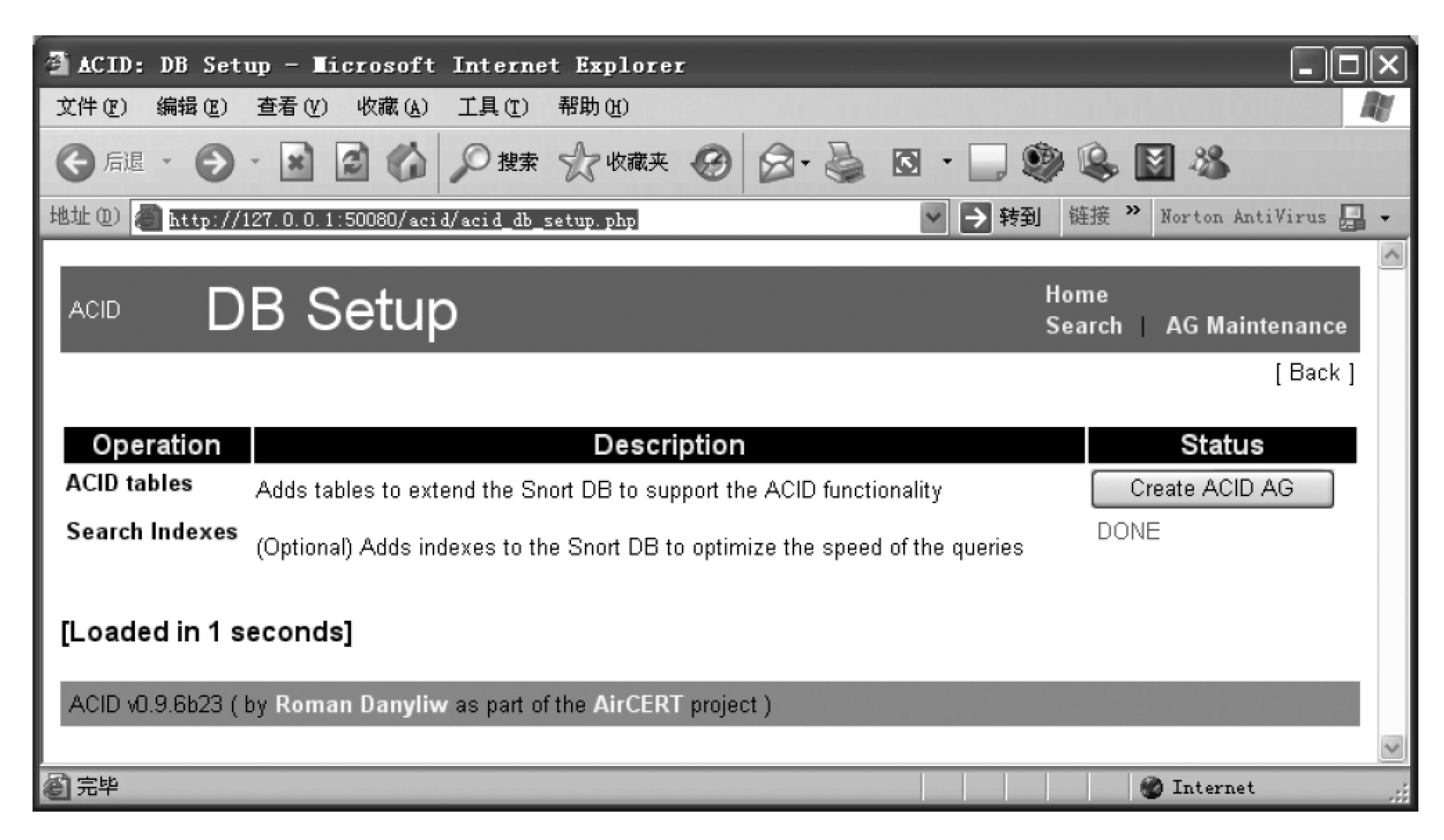


图 7.15　ACID 启动界面

测试 Snort 是否正常：C:\>snort -dev，能看到一只正在奔跑的小猪证明工作正常，如图 7.16 所示。

```
c:\Snort\bin>snort -dev
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "\Device\NPF_{0DCADDAC-C810-411C-9F17-1D4BB64C9B1
C}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.0.1-ODBC-MySQL-FlexRESP-WIN32 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
eam
           Copyright (C) 1998-2010 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

Commencing packet processing (pid=2320)
```

图 7.16　Snort 启动界面

查看本地网络适配器编号：C:\>snort -W，正式启动 Snort：

```
C:\> cd snort\bin
C:\Snort\bin> snort –c "C:\Snort\etc\snort.conf" –i "C:\Snort\log" –d –e –X
```

（注意，其中-i 后的参数为网卡编号，由 snort -W 查看得知。）

```
C:\Snort\bin> snort –c "C:\Snort\etc\snort.conf" –l "C:\Snort\logs" –i 2 –d –e –X
```

- -X 参数：用于在数据链接层记录 raw packet 数据。
- -d 参数：记录应用层的数据。
- -e 参数：显示/记录第二层报文头数据。

• -c 参数：用于指定 Snort 的配置文件的路径。
• -i 参数：指明监听的网络接口。

在 CMD 中，运行 snort -W，W 大写。此命令可以作为 Snort 是否安装成功的标志，同时可以看到运行着的网卡信息。一般情况下，snort -v 就可以实现简单的嗅探任务。Ctrl+C 结束嗅探。

较复杂的是配置。RULE_PATH、SO_RULE_PATH、PREPROC_RULE_PATH、dynamicpreprocessor 和 dynamicengine 的路径设置必须是绝对路径。有一点需要留意，dynamicpreprocessor 的路径最后不要以斜杠或反斜杠结尾，如果有会造成引擎加载失败。

使用配置的命令方式为：snort -v -c "C:\Snort\etc\snort.conf"，按此命令，若出现“ERROR：OpenAlertFile ( ) = > fopen ( ) alert file log/alert.ids：No such file or directory”，可通过 snort -l C:\Snort\mylogs -c C:\Snort\etc\snort.conf 将文件写入指定目录中。

打开 http://localhost:50080/acid/acid_main.php 网页，进入 ACID 分析控制台主界面，可以查看入侵检测的结果，如图 7.17 所示。

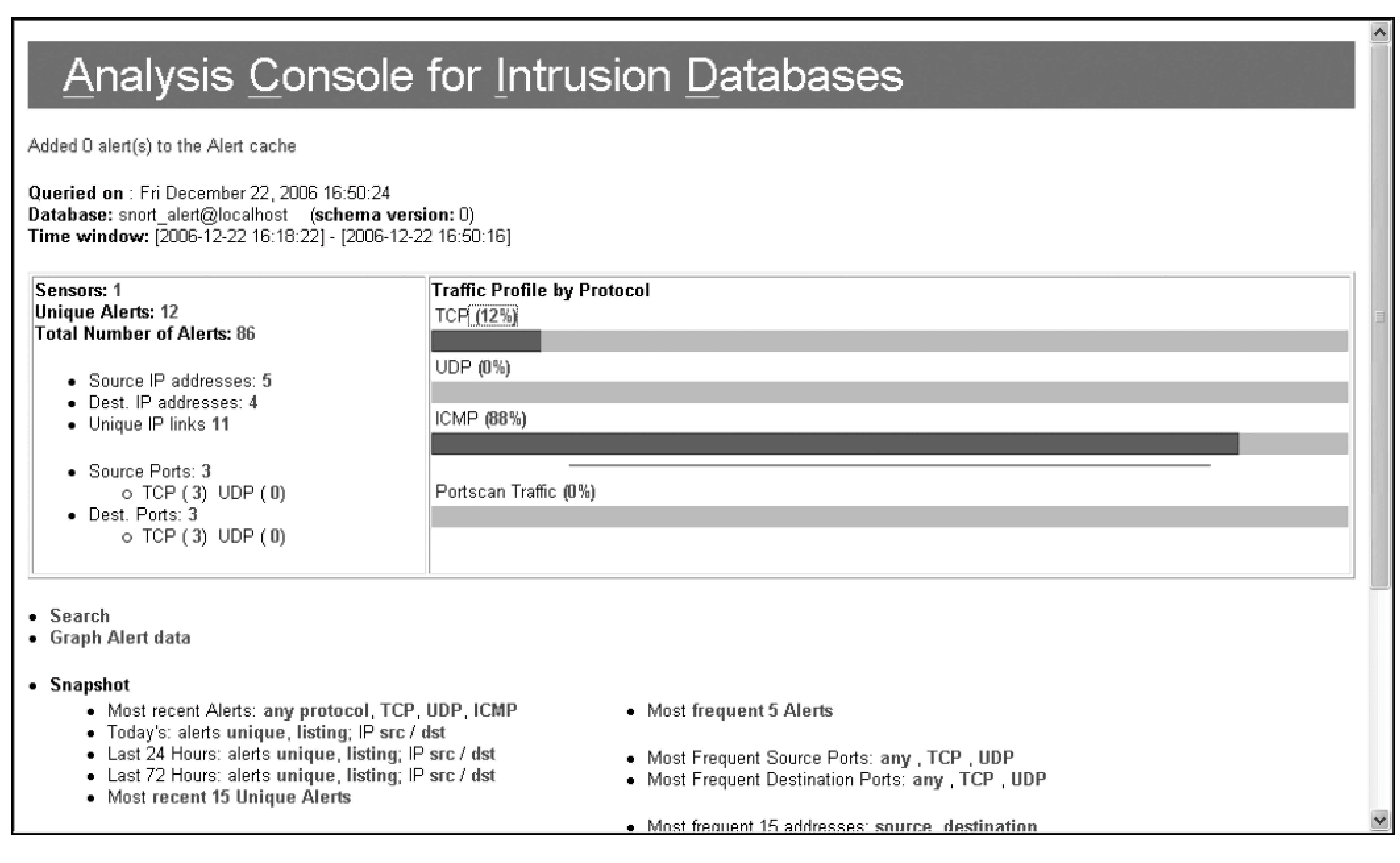


图 7.17 ACID 显示 Snort 的检测结果

利用扫描实验的要求扫描局域网，查看检测的结果。

安装 Snort 时注意关闭防火墙。

Appach 启动命令：apache -k install 或| apache -k start。

实验报告要求

• 实验目的。
• 附上实验过程的截图和结果截图。
• 阐述碰到的问题以及解决方法。

- 阐述收获与体会。

7.3 Snort 扩展实验

实验器材

- Snort 软件系统 1 套。
- PC(Windows XP/Windows 7)1 台。

预习要求

- 做好实验预习,复习入侵检测技术的有关内容。
- 熟悉 Snort 软件的使用方法。
- 熟悉实验过程和基本操作流程。
- 做好预习报告。

实验任务

通过本实验,进一步熟悉和掌握 Snort 系统,完善入侵检测技能。

实验环境

装有 Windows XP/Windows 7 操作系统的 PC 一台。

预备知识

入侵检测原理。

实验步骤

1. 完善配置文件

打开 C:/Snort/etc/snort.conf 文件,查看现有配置。设置 Snort 的内、外网检测范围。将 snort.conf 文件中 var HOME_NET any 语句中的 any 改为自己所在的子网地址,即将 Snort 监测的内网设置为本机所在局域网。如本地 IP 为 192.168.1.10,则将 any 改为 192.168.1.0/24,并将 var EXTERNAL_NET any 语句中的 any 改为 !192.168.1.0/24,即将 snort 监测的外网改为本机所在局域网以外的网络。设置监测包含的规则。找到 snort.conf 文件中描述规则的部分,如图 7.18 所示,snort.conf 文件中包含的检测规则文件前面加 # 表示该规则没有启用,将 local.rules 之前的 # 号去掉,其余规则保持不变。

2. 使用控制台查看检测结果

打开 http://localhost/acid/acid_main.php 网页,启动 Snort 并打开 ACID 检测控制台主界面,如图 7.19 所示。

单击图示中 TCP 后的数字"80%",将显示所有检测到的 TCP 协议日志详细情况,如图 7.20 所示。TCP 协议日志网页中的选项依次为流量类型、时间戳、源地址、目标地址以及协议。由于 Snort 主机所在的内网为 202.112.108.0,可以看出,日志中只记录了外网 IP 对内网的连接(即目标地址均为内网)。

```
include $RULE_PATH/finger.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/telnet.rules
#include $RULE_PATH/rpc.rules
#include $RULE_PATH/rservices.rules
#include $RULE_PATH/dos.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
```

图 7.18 Snort 配置页面

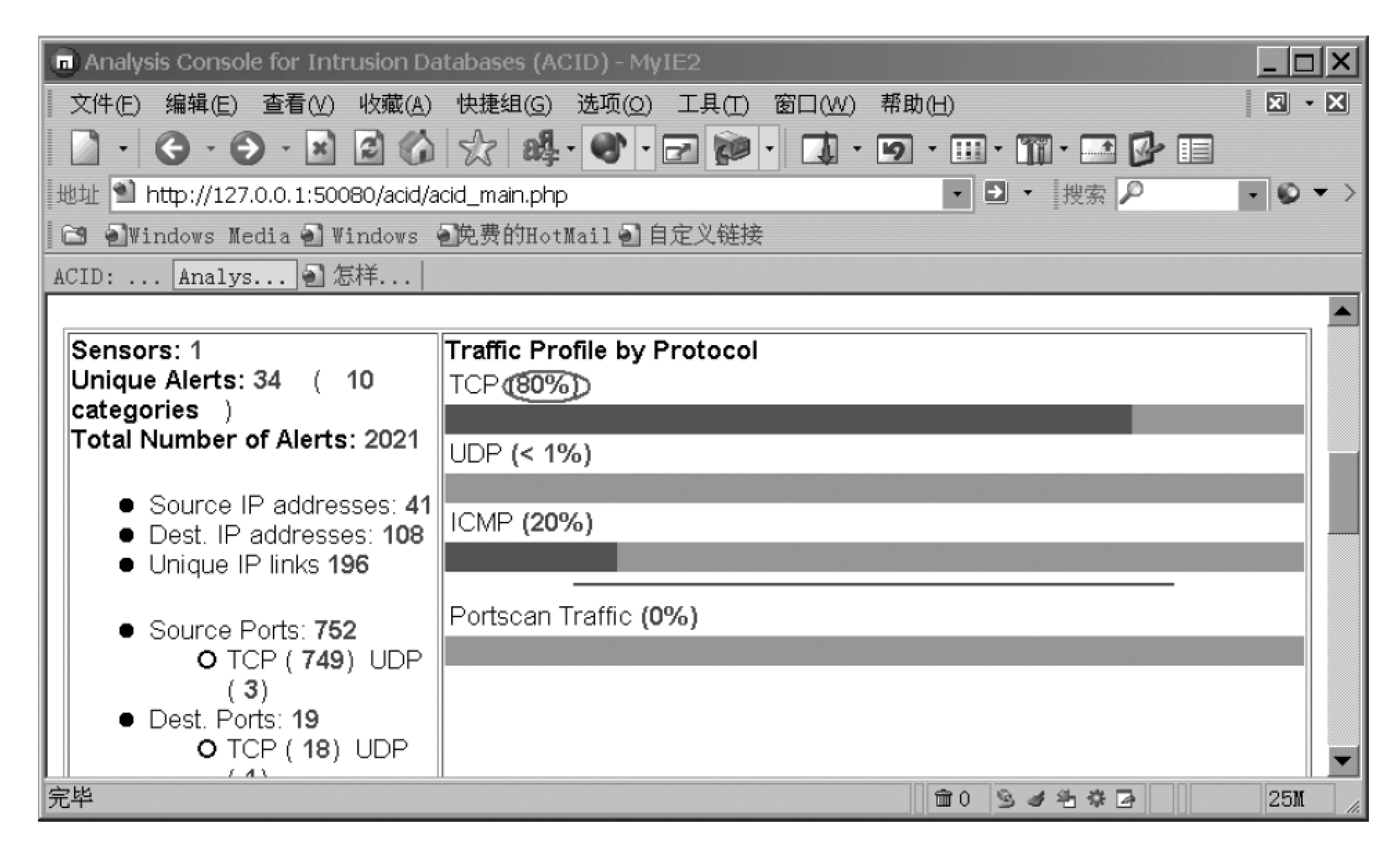


图 7.19 Snort 控制台页面

选择控制条中的 home 返回控制台主界面，在主界面的下部有流量分析及归类选项，如图 7.21 所示。

选择 Last 24 Hours：alerts unique，可以看到 24 小时内特殊流量的分类记录和分析，其中详细记录了各类型流量的种类、在总日志中所占的比例、出现该类流量的起始和终止时间等详细分析（在控制台主界面中还有其他功能，请自己练习使用）。

3. 配置 Snort 规则

练习添加一条规则，以对符合此规则的数据包进行检测，打开 C:\Snort\rules\local.rules 文件，如图 7.22 所示。

在规则中添加一条语句，实现对内网的 UDP 协议相关流量进行检测，并报警：udp ids/dns-version-query。语句如下：

```
alert udp any any<>$HOME_NET any(msg:"udp ids/dns-version-query";content:"version";)
```

保存文件后，退出。重启 Snort 和 ACID 检测控制台，使规则生效。

实验报告要求

- 实验目的。

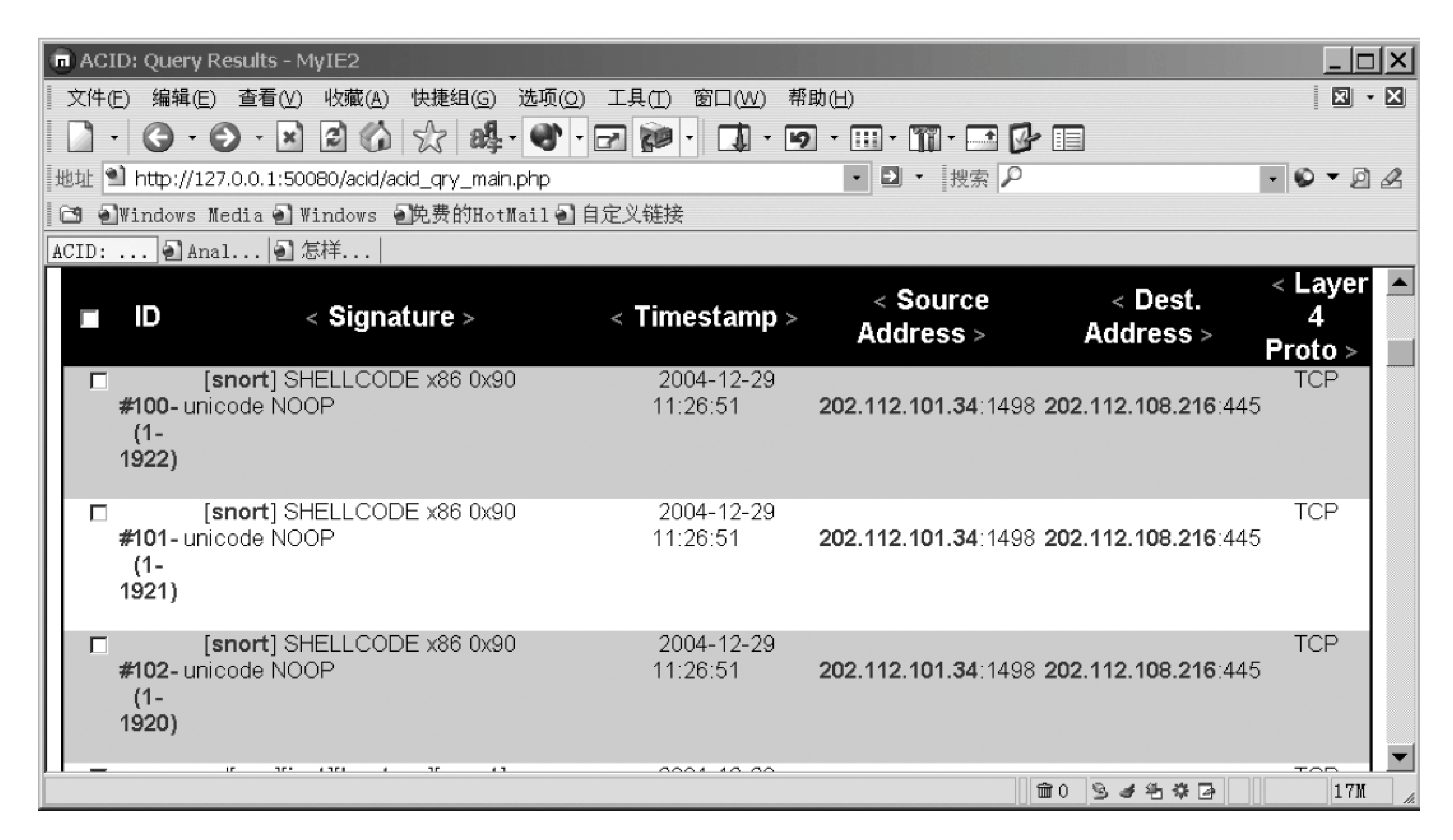


图 7.20　Snort 结果检测页面

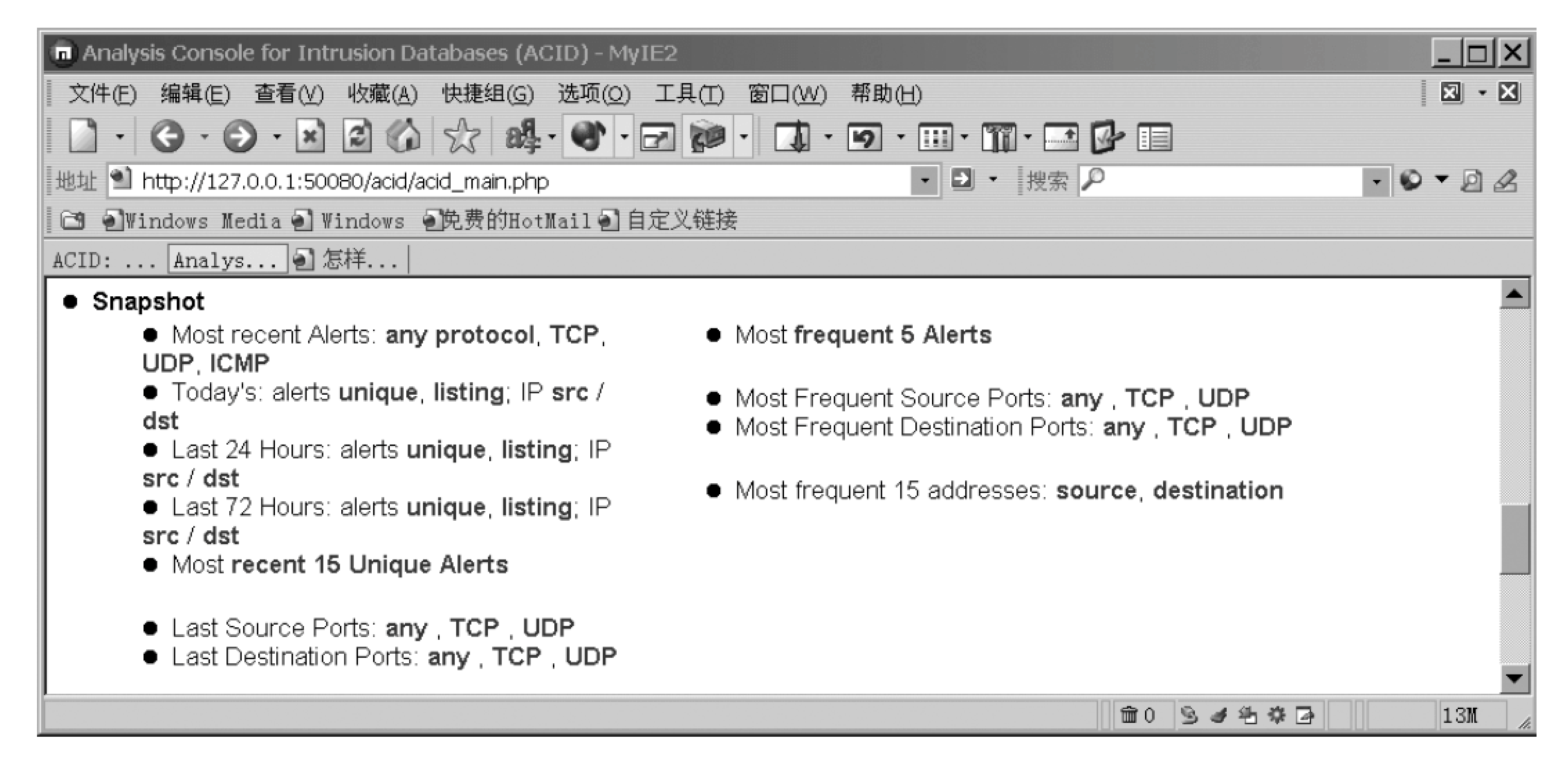
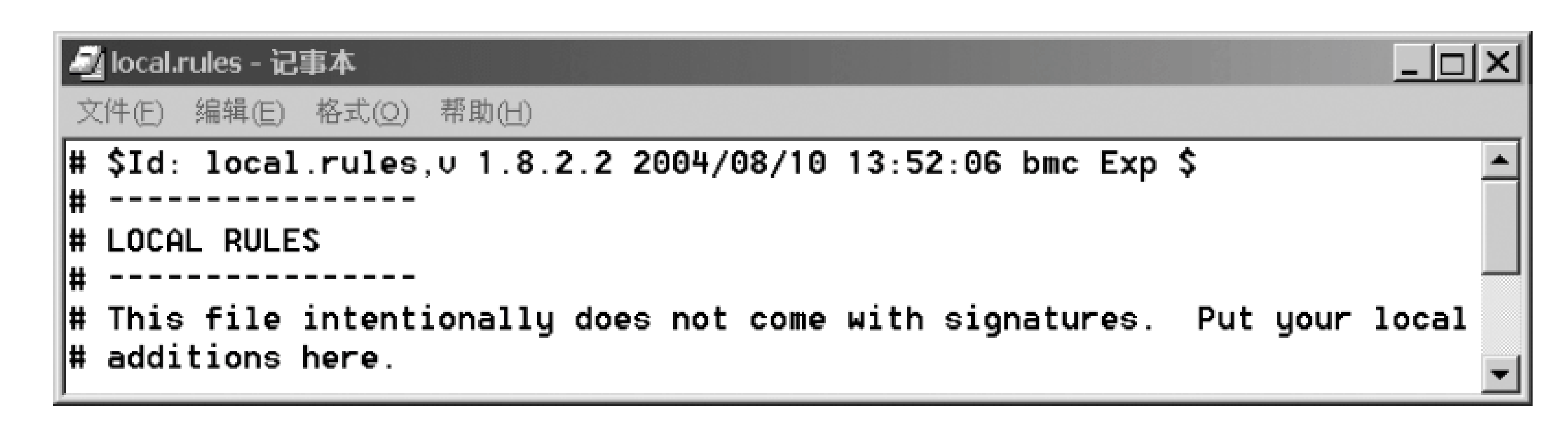


图 7.21　Snort 控制台检测页面



```
# $Id: local.rules,v 1.8.2.2 2004/08/10 13:52:06 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
```

图 7.22　Snort 规则编辑文件

- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。

- 阐述收获与体会。

第 8 章　虚拟蜜网实验

8.1　虚拟蜜网系统

8.1.1　蜜网技术

蜜网技术作为一种新兴的网络安全技术,已经得到国外很多研究机构和公司的重视。蜜网技术的发展可以概括为以下几个阶段。

- 蜜网早期(1999 年至 2001 年):这一阶段的研究关注于验证蜜网理论,试验蜜网模型。在此期间建立了第一代蜜网模型。
- 蜜网中期(2002 年至 2004 年):这一阶段的核心研究内容是简化蜜网应用。中期将改进蜜网的易用性作为研究的重点。在此期间建立了第二代蜜网模型,增强了蜜网的易用性,还出现了虚拟蜜网技术和分布式的多蜜网构架。
- 目前,蜜网的研究重点是增强蜜网的隐蔽性和易用性。

我国在该领域的研究开始较晚。2001 年国家自然科学基金信息安全项目正式对该领域进行了立项研究。2005 年 1 月北京大学的“狩猎女神”计划是我国第一个专门针对蜜网技术的研究项目,同年 2 月该研究小组正式加入世界蜜网联盟。

蜜网(honeynet)是一种用来被攻击或攻陷的网络资源,它不是一个单一的系统,而是一个让入侵者攻击的网络架构。蜜网装有多个系统和应用软件,所有放置在蜜网内的系统都是标准的产品系统,而不是仿效的操作系统和应用软件。

蜜网的三大核心功能是数据控制、数据捕获和数据集中。

- 数据控制功能能够防止攻击者利用蜜网系统危害第三方网络的安全,从而降低蜜网的使用风险。
- 数据捕获功能能够捕获入侵者的所有攻击行为数据。
- 数据集中功能便于多个蜜网的集中管理和数据分析。

8.1.2　虚拟蜜网

虚拟蜜网和传统蜜网具有相同功能,能够在单个主机上运行传统蜜网的所有组成部分,这使得蜜网部署更加便捷,配置更加集中。虚拟蜜网与单机蜜罐相比更加复杂高效,提高了蜜罐系统检测、响应、恢复和分析受侵害系统的能力。

8.1.2.1　虚拟蜜网种类

虚拟蜜网分为两类:独立型虚拟蜜网和混杂型虚拟蜜网。

1. 独立型虚拟蜜网

独立型虚拟蜜网就是在一台物理主机上实现整个蜜网系统,包括具有数据控制和数据捕获功能的蜜网网关以及蜜网中的蜜罐,如图 8.1 所示。

独立型虚拟蜜网的优点：便携性；廉价的空间开销。

独立型虚拟蜜网的缺点：需要高性能硬件配置；安全性极大程度上依赖于虚拟软件；由于物理主机的硬件限制，很难实现对所需操作系统的完美模拟。

2. 混杂型虚拟蜜网

混杂型虚拟蜜网是一种同时使用蜜网网关和虚拟软件实现蜜网系统的方案。数据捕获（如防火墙）、数据控制（如 IDS）和日志系统都放在一个独立、隔离的系统中，而所有蜜罐都运行在另一个主机的虚拟空间中，这种方案减少了虚拟蜜网的风险，如图 8.2 所示。

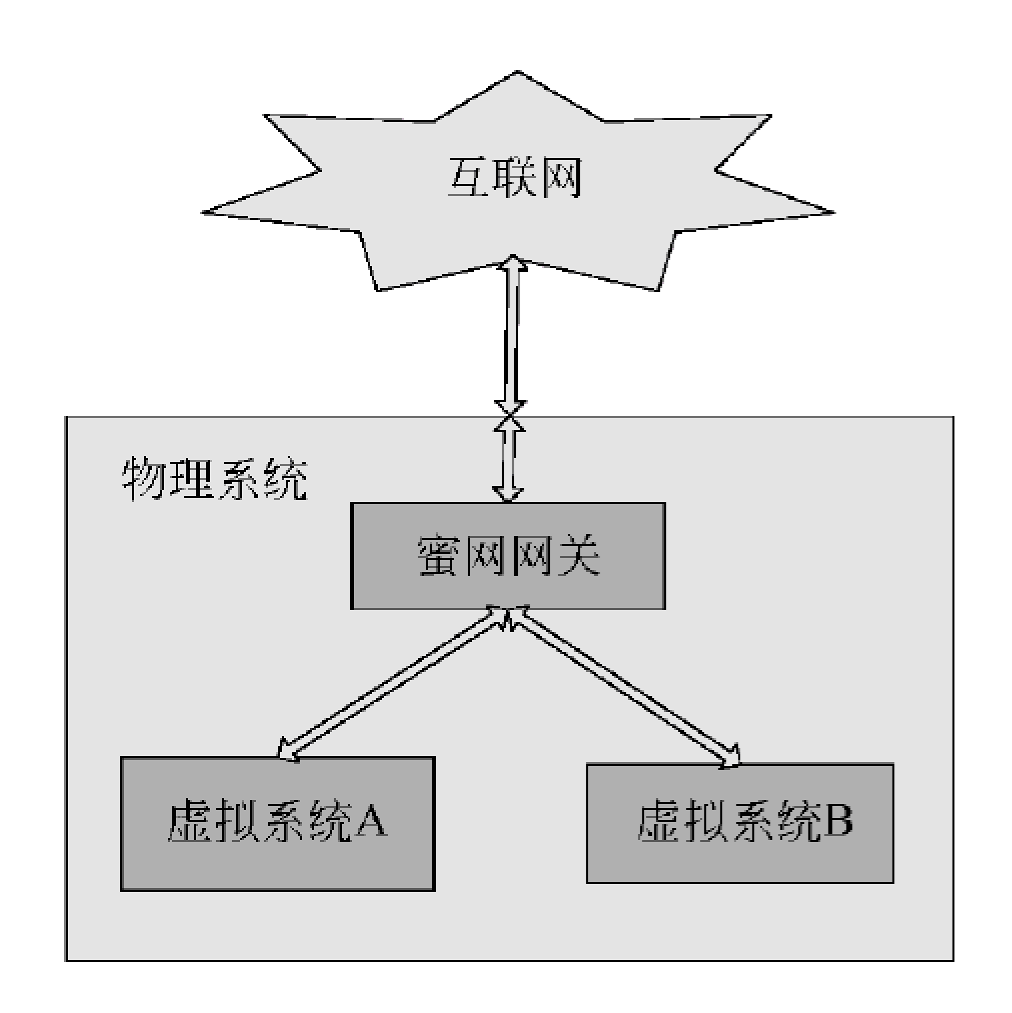


图 8.1 独立型虚拟蜜网结构

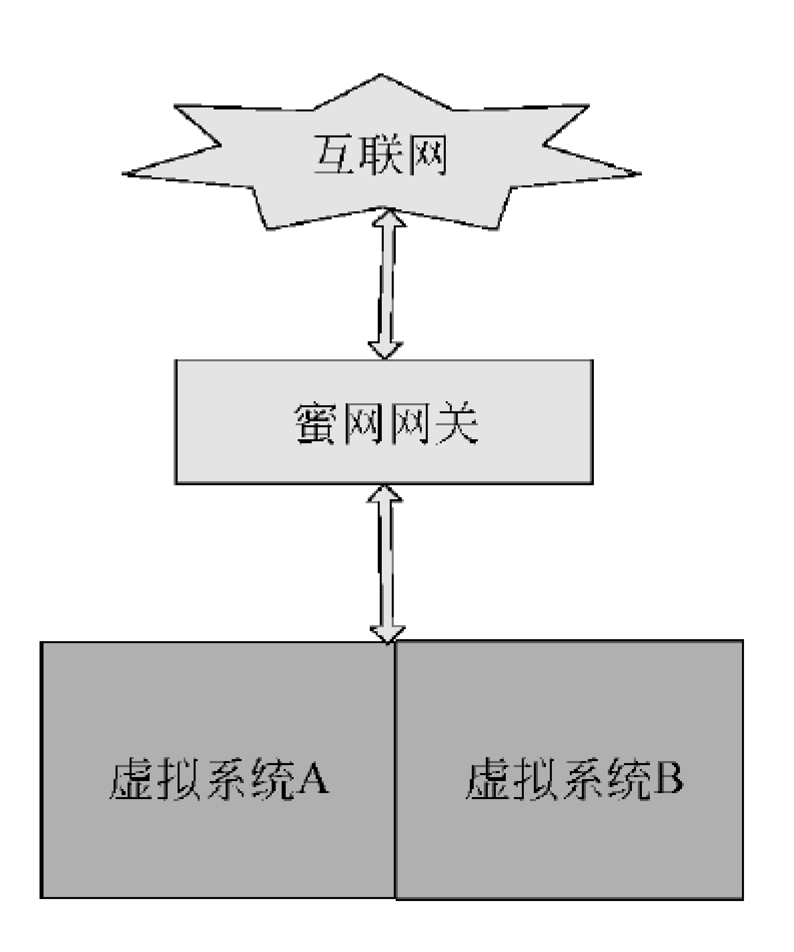


图 8.2 混杂型虚拟蜜网系统结构

混杂型虚拟蜜网的优点：安全性和灵活性；入侵者仅可能入侵虚拟蜜罐；可以根据需要运行任意种类的蜜罐。

混杂型虚拟蜜网的缺点：不易移动；便携性不强；需要较高的费用和空间开销。

8.1.2.2 蜜网实现方式

虚拟蜜网的实现方法主要有三种：VMware Workstation、VMware GSX Server 和 User Mode Linux。

1. VMware Workstation

VMware Workstation 是一个虚拟机软件，可以运行在 Linux 和 Windows 两种平台下，模拟主板、内存、硬盘、网卡、声卡、USB 口等多种硬件。VMware Workstation 是目前搭建虚拟蜜网的最佳选择，设计对象主要为桌面用户，功能强大。

VMware Workstation 具有以下特性：

- 支持多种操作系统。虚拟环境中可以运行的操作系统包括 Linux、Solaris、Windows 和 FreeBSD 等。
- 提供两种联网方式：一是为独立型虚拟蜜网提供的桥接方式；一是为独立型虚拟蜜网提供的 Host-Only 联网方式。
- 支持镜像功能。为每个虚拟蜜罐提供镜像文件，方便了蜜罐的移植和备份，并具有加载虚拟磁盘镜像的功能。
- 具有较好的技术支持、升级和补丁等服务和方便易用的图形接口。

2. VMware GSX Server

VMware GSX Server 是 VMware Workstation 的服务器增强版本，可以运行更多复杂的服务。VMware GSX Server 一般将 Linux 和 Windows 作为宿主操作系统。VMware 公司还有一种 ESX Server 服务器版本，不但提供软件解决方案，而且提供一定的硬件解决方案。

3. User Mode Linux

UML 具有在一个系统上同时运行多个 Linux 实例的能力。它是一种相对较新的工具，具有很大的发展潜力。

User Mode Linux 具有以下特性：

- 开放公开的源代码，可以根据需要修改 UML 源代码。
- 可供“指纹”识别的信息较少，资源要求较少。
- 可以构建多个虚拟网络，并且能够在虚拟网络里创建虚拟路由器。
- 支持桥接和 Host-Only 两种联网方式。
- 支持操作系统内核记录击键序列功能。
- 可通过预先配置好的可下载的文件系统方式来实现虚拟蜜罐。
- 支持多种方式访问 UML 控制台，包括使用伪终端、xterm、通过 Telnet 方式进入的入口，甚至通过屏幕方式。

UML 目前仅支持 Linux 虚拟机器，而且 UML 还存在很多程序漏洞、文档和安全问题，由于 UML 没有 GUI 图形界面，现在所有配置和实现都必须在命令行下完成，不易使用。

8.2 搭建虚拟蜜网

实验器材

- 虚拟蜜网软件综合系统 1 套。
- PC(Windows XP/Windows 7)1 台。

预习要求

- 做好实验预习，复习虚拟蜜网技术的有关内容。
- 熟悉搭建虚拟蜜网的各类软件。
- 熟悉实验过程和基本操作流程。
- 做好预习报告。

实验任务

通过本实验，学会安装相关虚拟蜜网软件的方法，了解虚拟蜜网的搭建过程。

实验环境

操作系统为 Windows XP 的 PC 一台。

预备知识

- 蜜网技术。
- 虚拟蜜网原理。

实验步骤

1. 搭建工具介绍

VMware 软件主要有 VMware Player(免费)、VMware Workstation、VMware GSX Server(目前 License 免费)、VMware ESX Server 等版本,本实验使用的版本为 VMware Workstation 5.5.1-19175。

运行在 VMware 虚拟机软件上的操作系统的网络连接方式有三种。

(1) 桥接方式(Bridge):在桥接方式下,VMware 模拟一个虚拟网卡,主系统对于客户系统来说相当于是一个桥接器,客户系统对于外部直接可见,如图 8.3 所示。

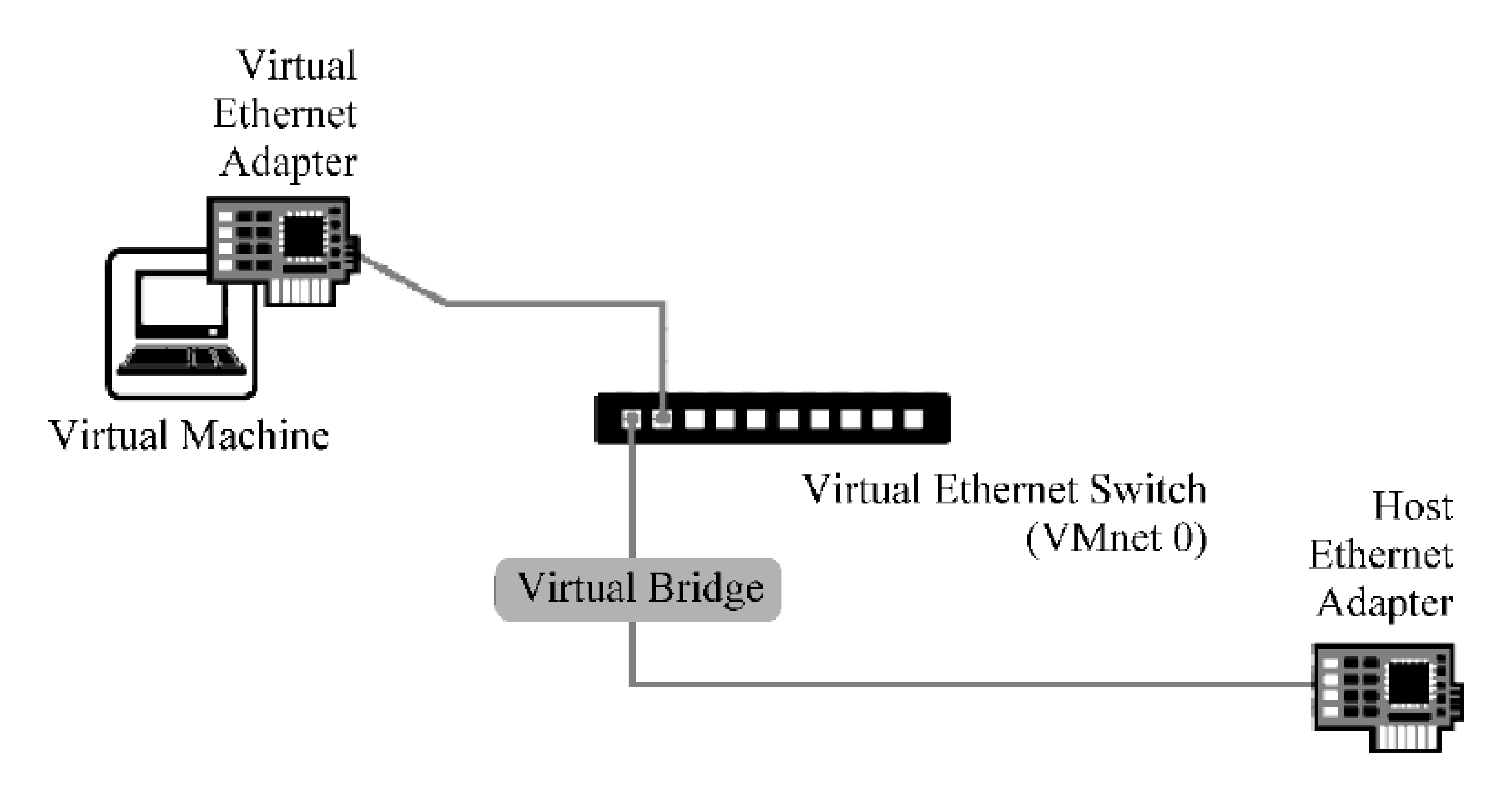


图 8.3 桥接方式

(2) 网络地址转换方式(NAT):客户系统不能直接连接网络,必须通过主系统对所有进出网络的客户系统收发的数据包做地址转换,客户系统对于外部不可见,如图 8.4 所示。

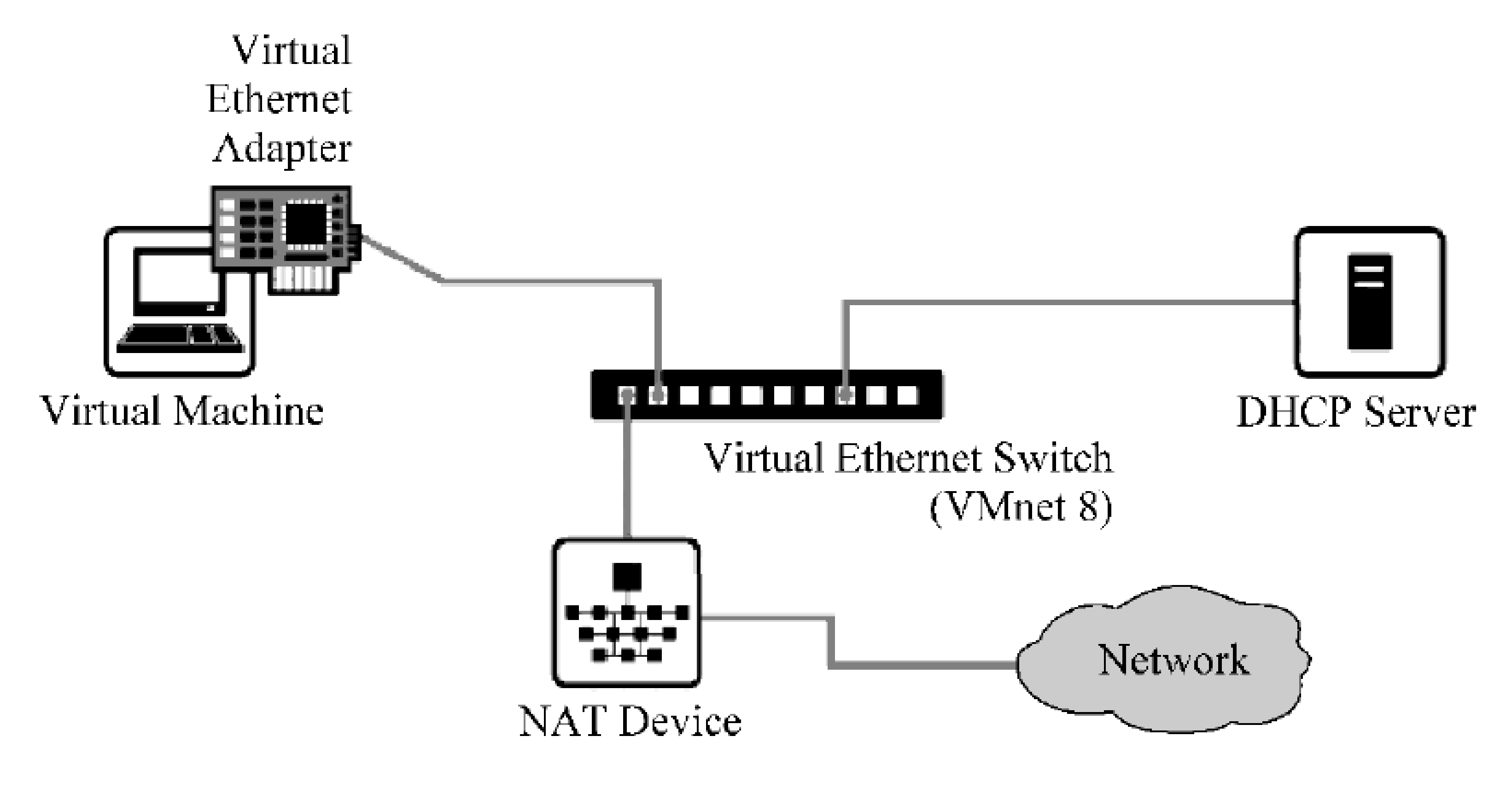


图 8.4 网络地址转换方式

(3) 主机方式(Host-Only):主系统模拟一个虚拟的交换机,所有客户系统通过这个交换机进出网络。如果主系统是用公网 IP 连接 Internet,那么客户系统只能用私有 IP。如果另外安装一个系统通过桥接方式连接 Internet,则这些客户系统的 IP 为公网 IP,直接从这个虚拟的桥接器连接 Internet,如图 8.5 所示。

若宿主主机只有一块网卡,可在该网卡上绑定多个 IP 地址,实际配置中将 IP 地址 192.168.0.2(攻击机 IP)和 192.168.1.2(控制机 IP)均绑定到宿主主机网卡上,如图 8.6 所示。

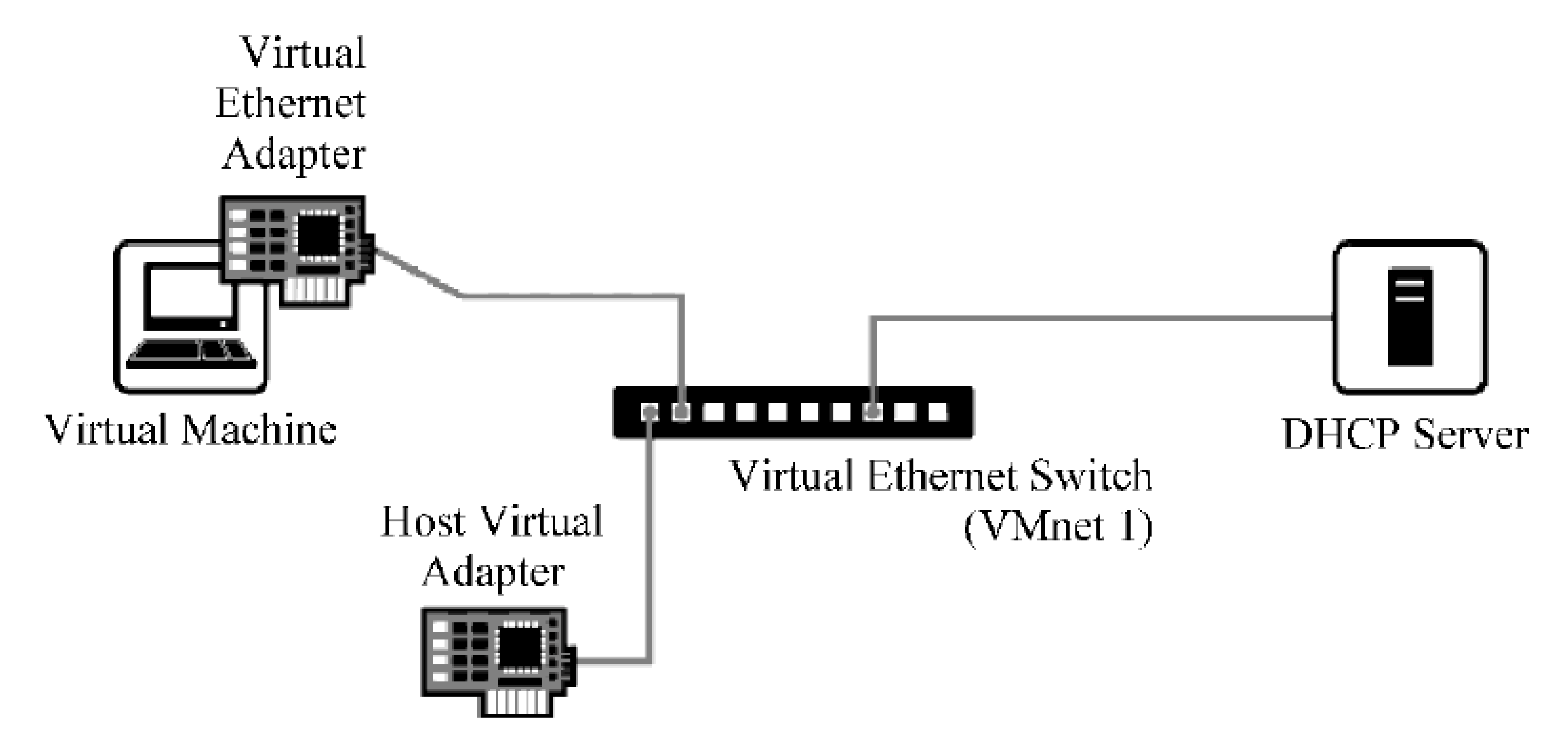


图 8.5　主机方式



图 8.6　网卡绑定设置

2. 环境配置

宿主主机：

- 操作系统：Windows 2000/Windows XP。
- VMware Workstation 5.5.1-19175。

蜜网网关虚拟机：

- Roo Honeywall CDROM v1.0-hw189。

蜜罐虚拟机：

- Windows 2000 Pro。

3. 系统搭建

(1) 以默认方式安装 VMware Workstation 软件。

(2) 安装蜜网网关虚拟机。

首先，新建虚拟机，选择 Custom 安装类型，如图 8.7 所示。

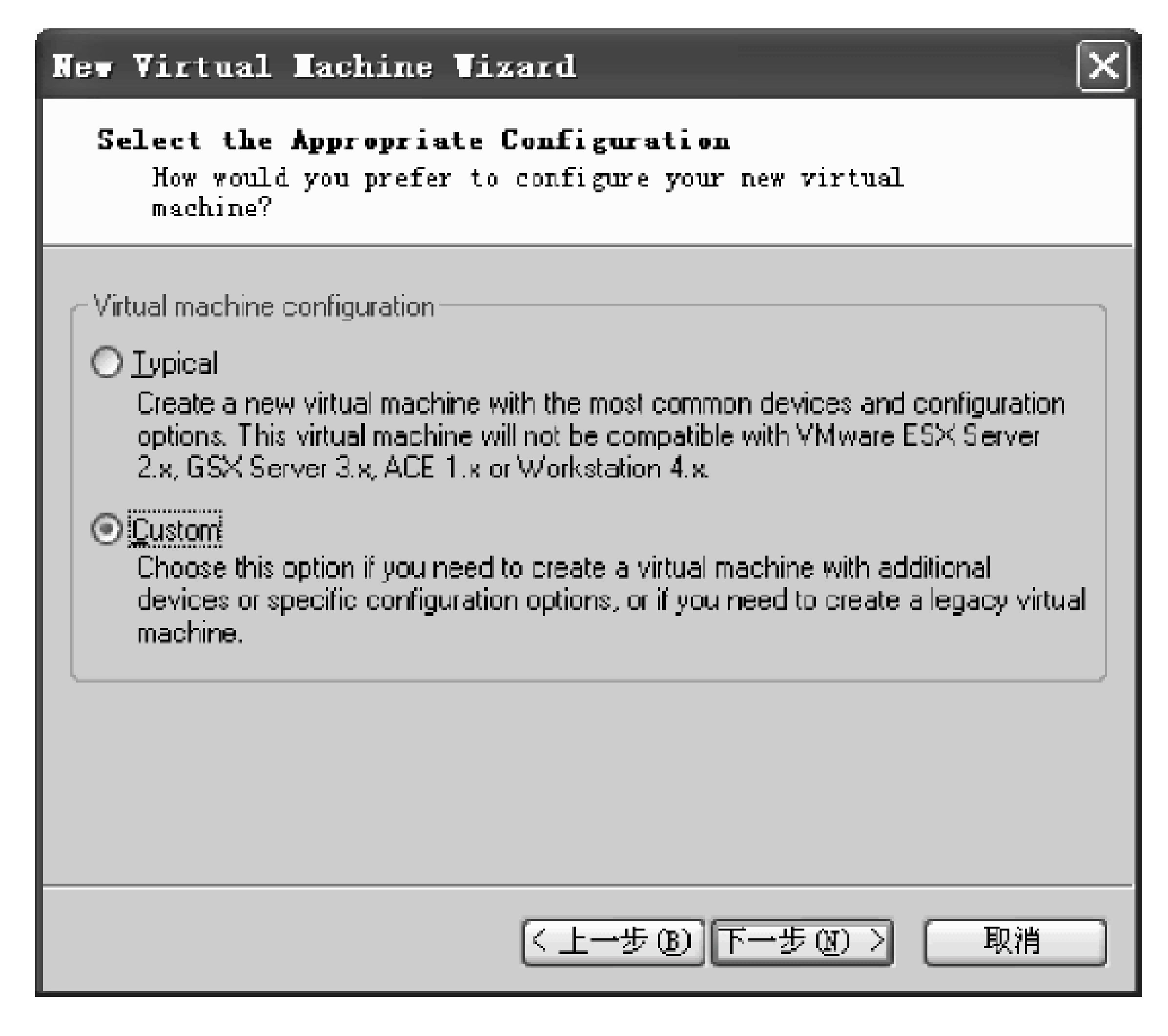


图 8.7　虚拟机安装界面

其次，选择蜜网网关虚拟机的操作系统类型，如图 8.8 所示。操作系统选择 Linux，版本选择 Red Hat Linux。

New Virtual Machine Wizard
Select a Guest Operating System
Which operating system will be installed on this virtual machine?
Guest operating system
Microsoft Windows
Linux
Novell NetWare
Sun Solaris
Other
Version
Red Hat Linux
< 上一步(B)
下一步(N) >
取消

图 8.8　操作系统选择界面

接下来，设置蜜网网关虚拟机命名与路径，如图 8.9 所示。

设置蜜网网关虚拟硬件，如图 8.10 所示。

设置蜜网网关虚拟机内存大小，建议设为 256MB，如图 8.11 所示。

设置网络连接方式，选择 Use bridged networking(桥接模式)，需另加两个网卡，如图 8.12 所示。

设置虚拟硬盘接口类型，SCSI 接口选择 BusLogic，如图 8.13 所示。

创建虚拟硬盘，如图 8.14 所示。

设置虚拟硬盘为 SCSI，如图 8.15 所示。

设置虚拟硬盘大小为 4GB，无需立即分配全部空间，如图 8.16 所示。

指定虚拟硬盘文件绝对路径，注意必须给出完整路径，不要出现中文字符，如图 8.17 所示。

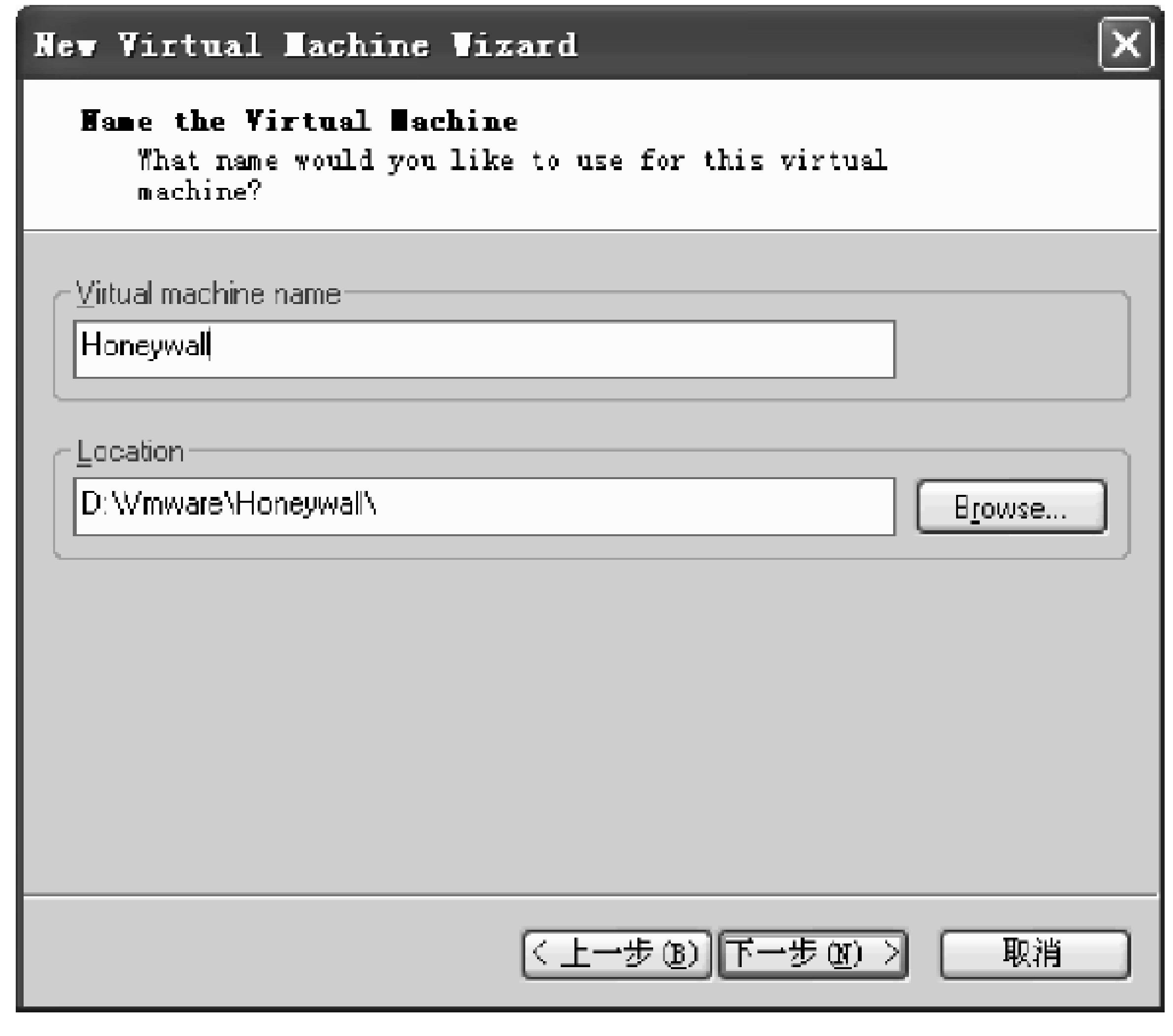


图 8.9 网关虚拟机设置界面

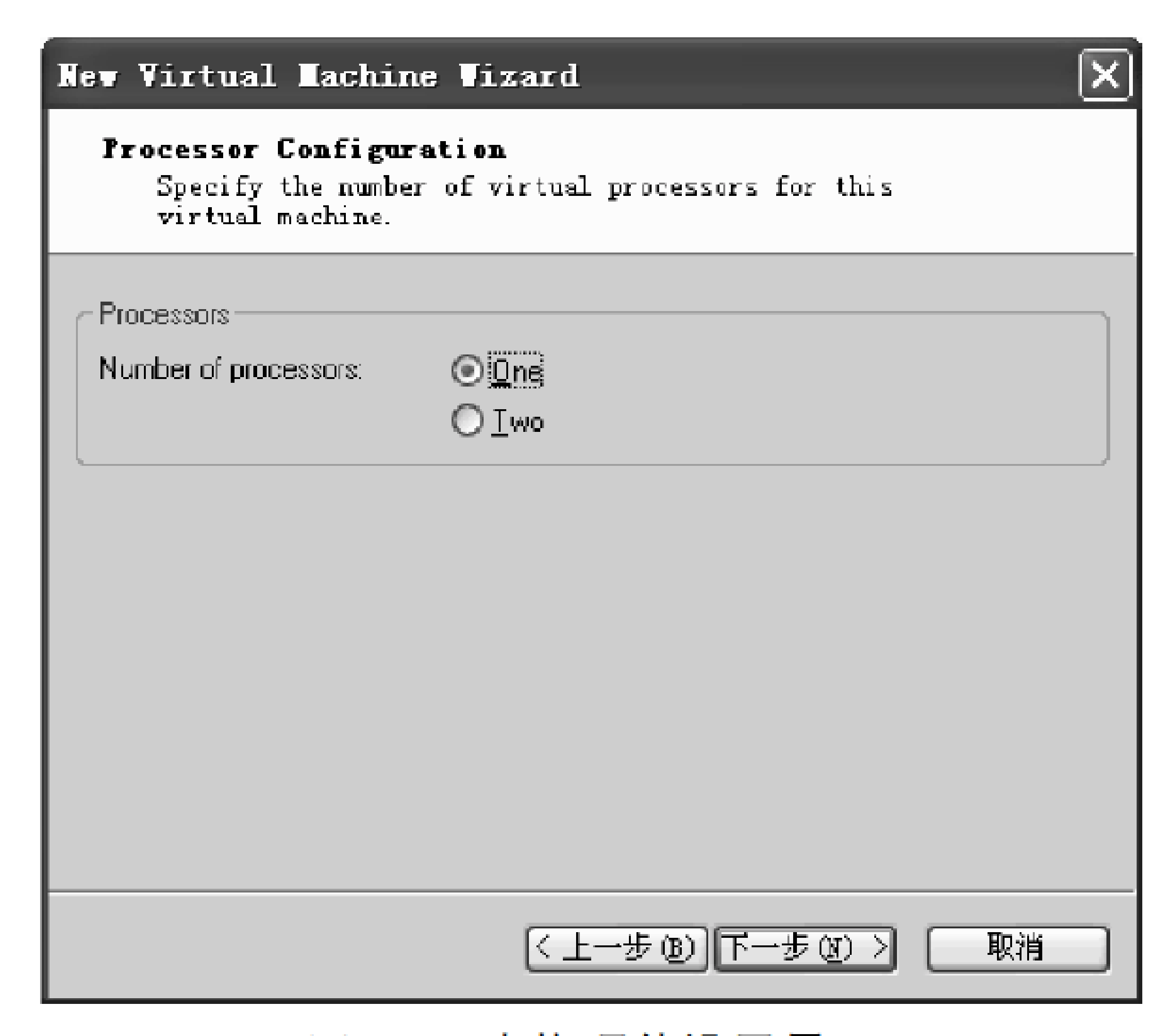


图 8.10 虚拟硬件设置界面

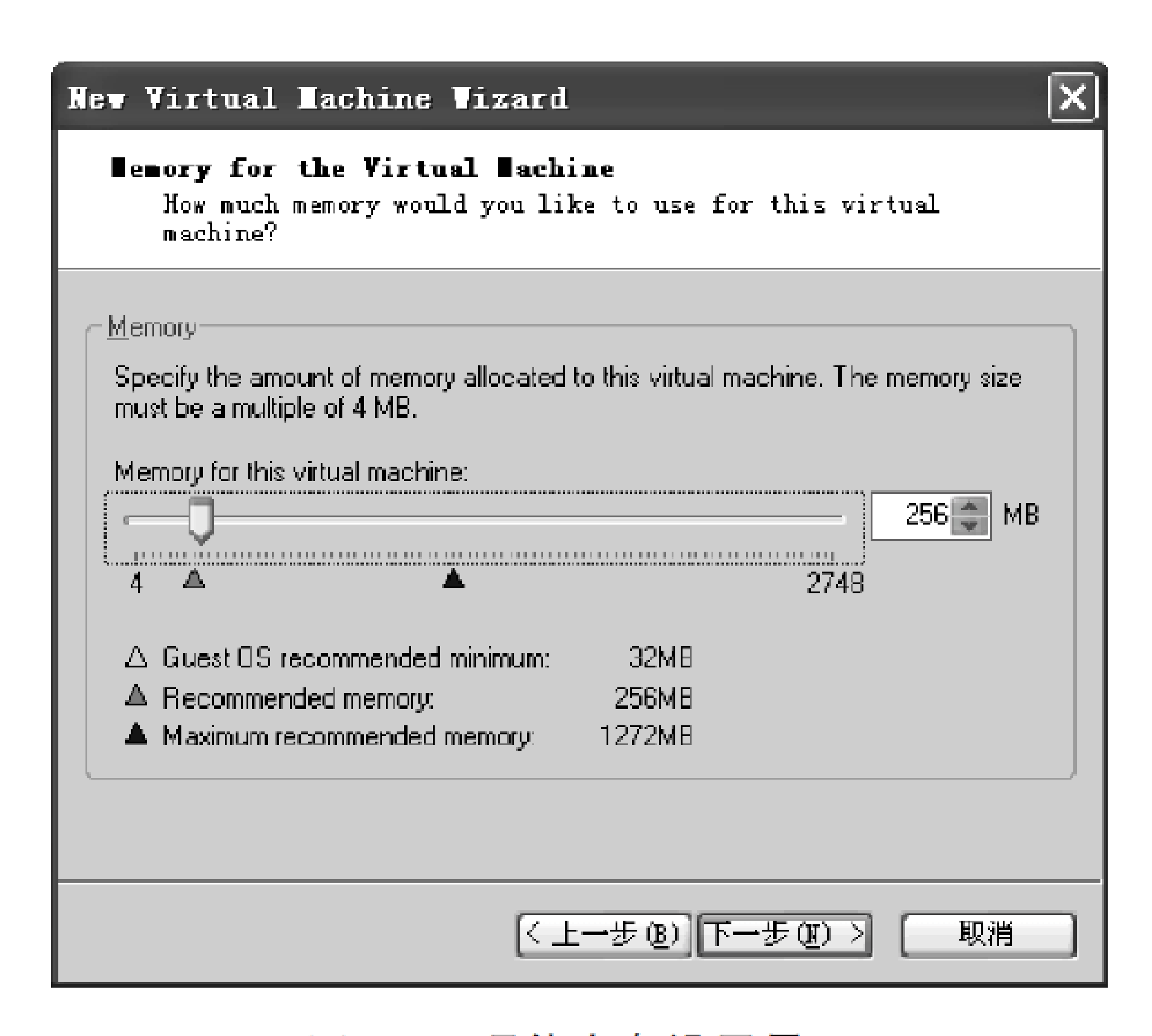


图 8.11 硬件内存设置界面

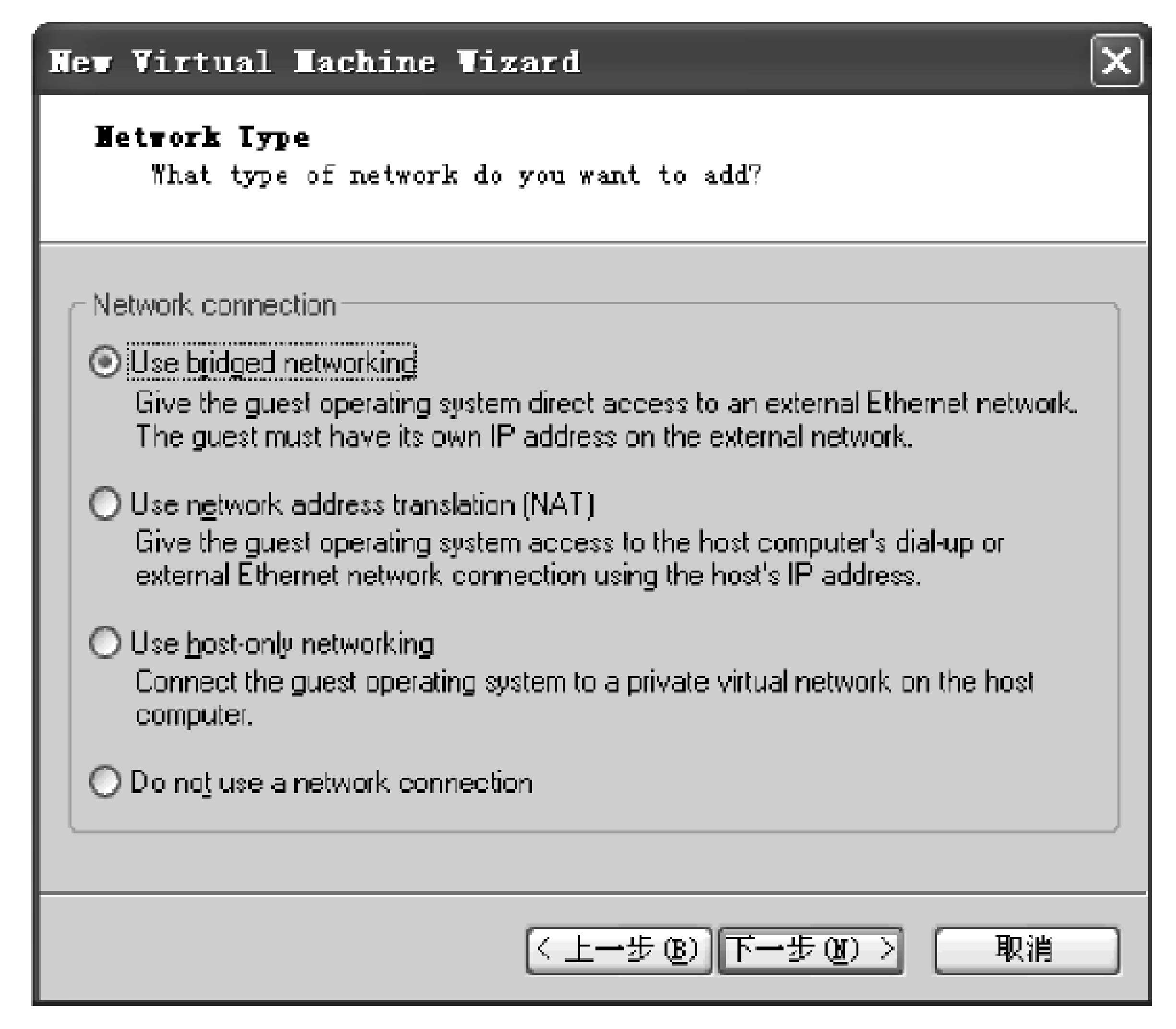


图 8.12　网络连接类型设置界面

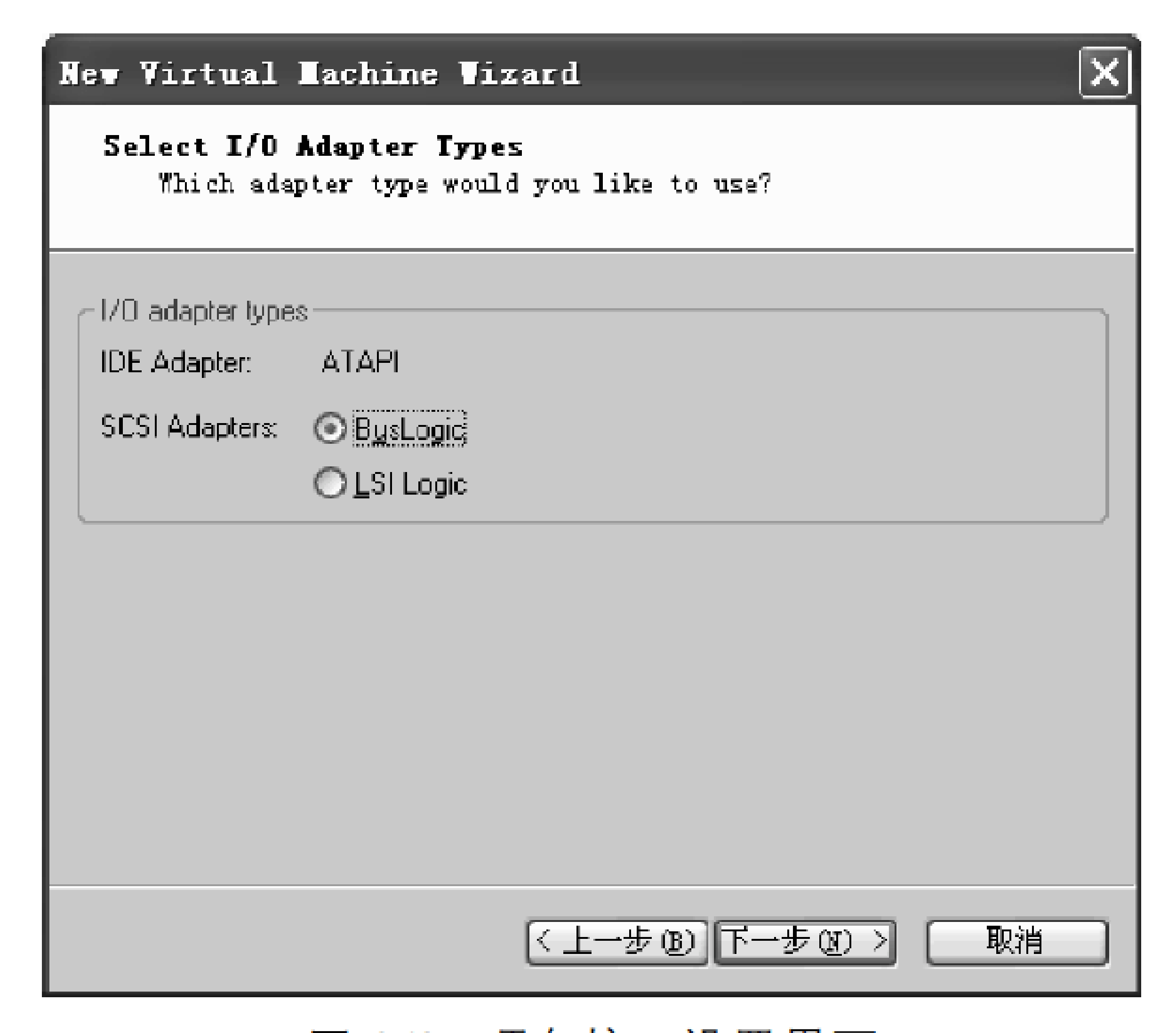


图 8.13　硬盘接口设置界面

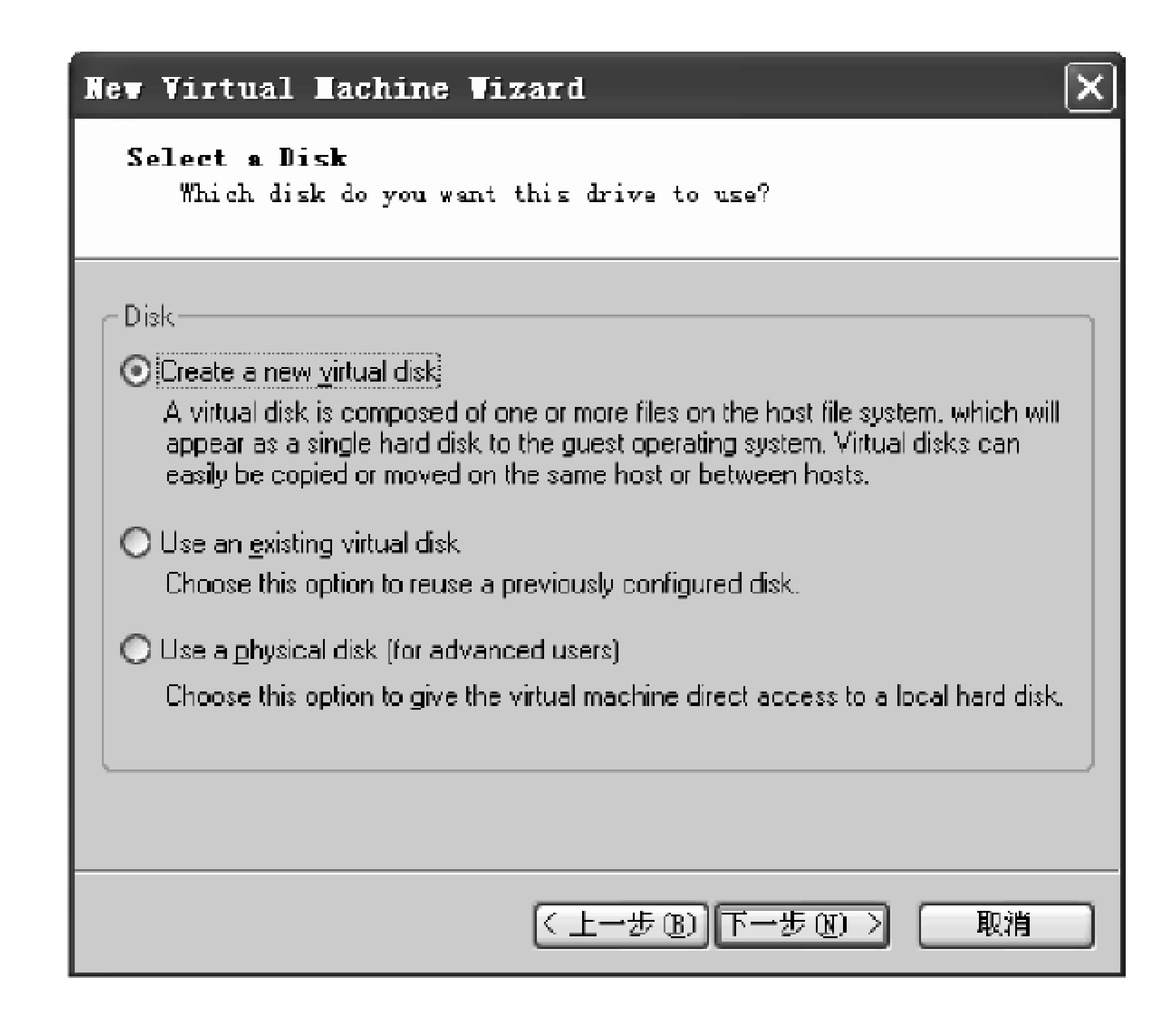


图 8.14　创建虚拟硬盘

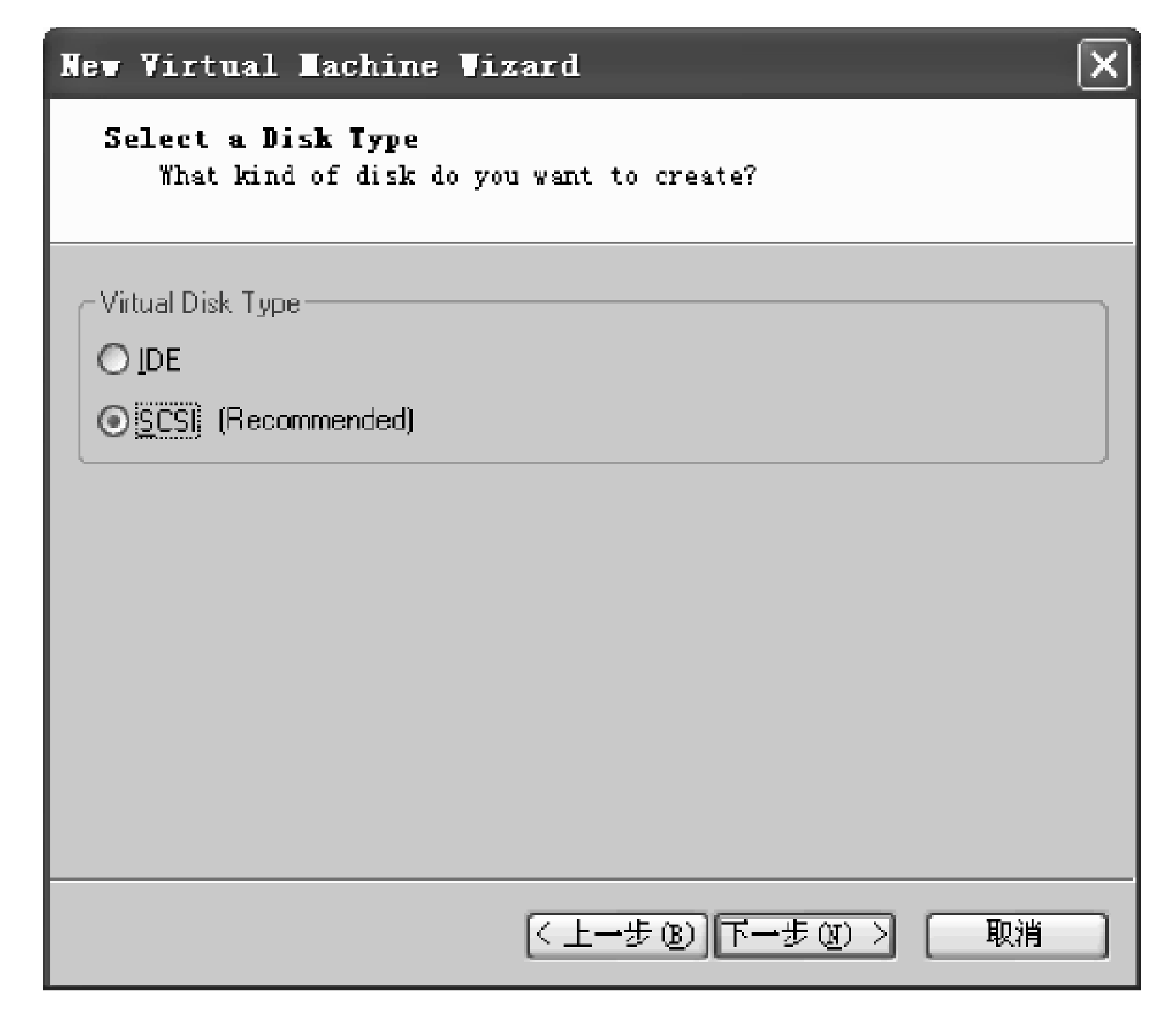


图 8.15 虚拟硬盘类型

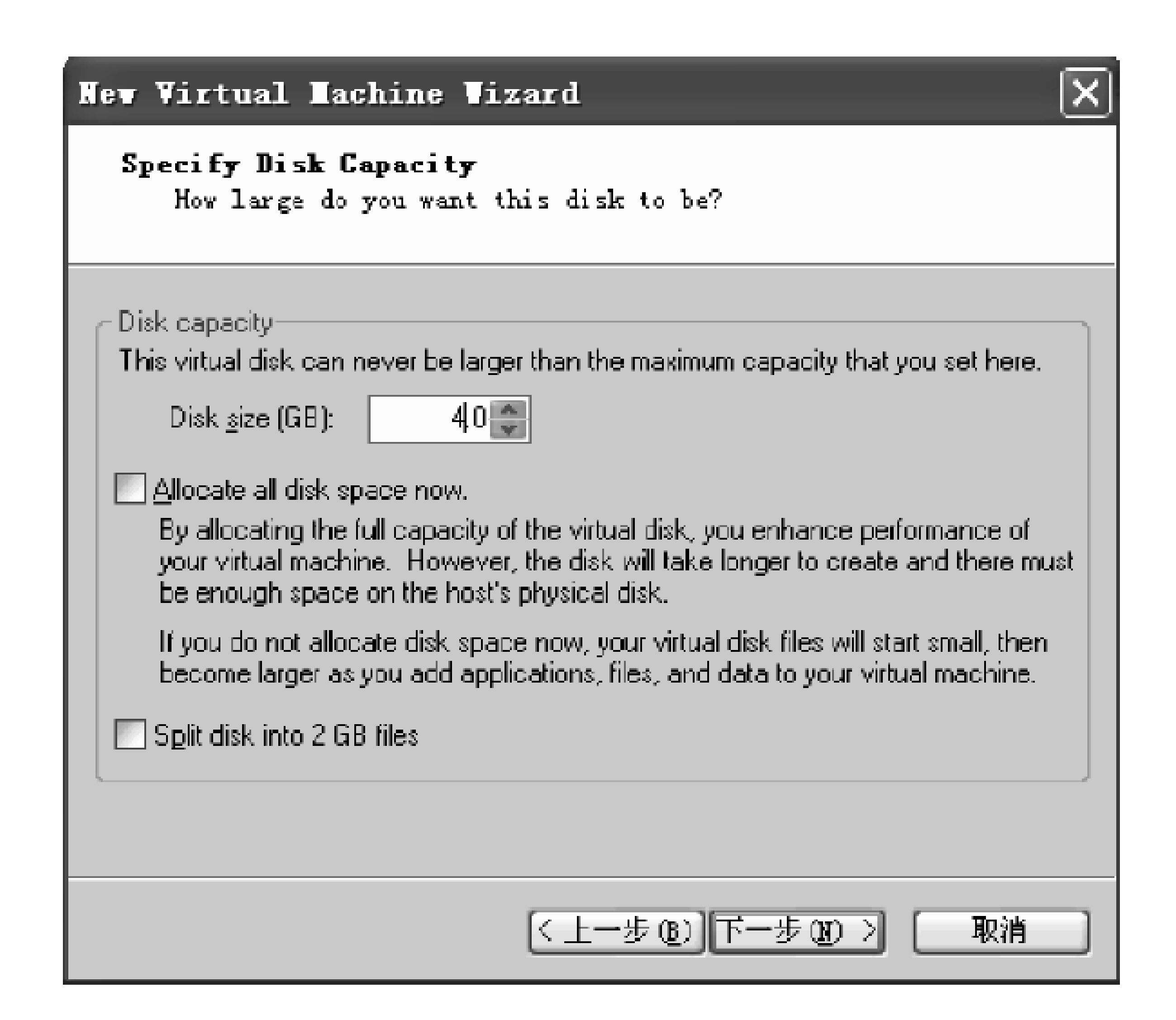


图 8.16 指定硬盘容量

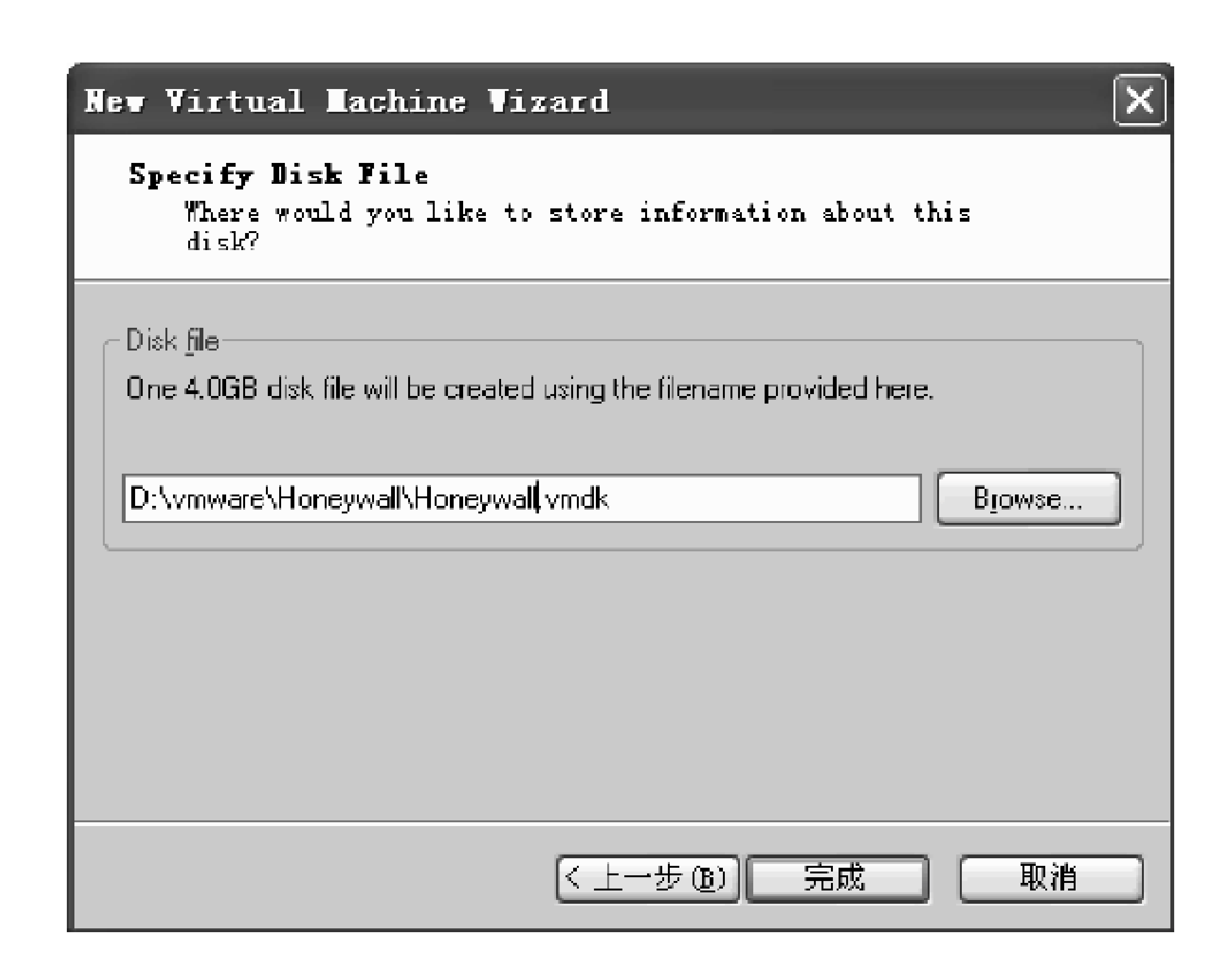


图 8.17 文件存储路径

接下来，需要对虚拟机进行具体配置，添加两块网卡，如图 8.18、图 8.19 所示，其中，Ethernet 2 设为 Host-only，Ethernet 3 设为 Bridged。

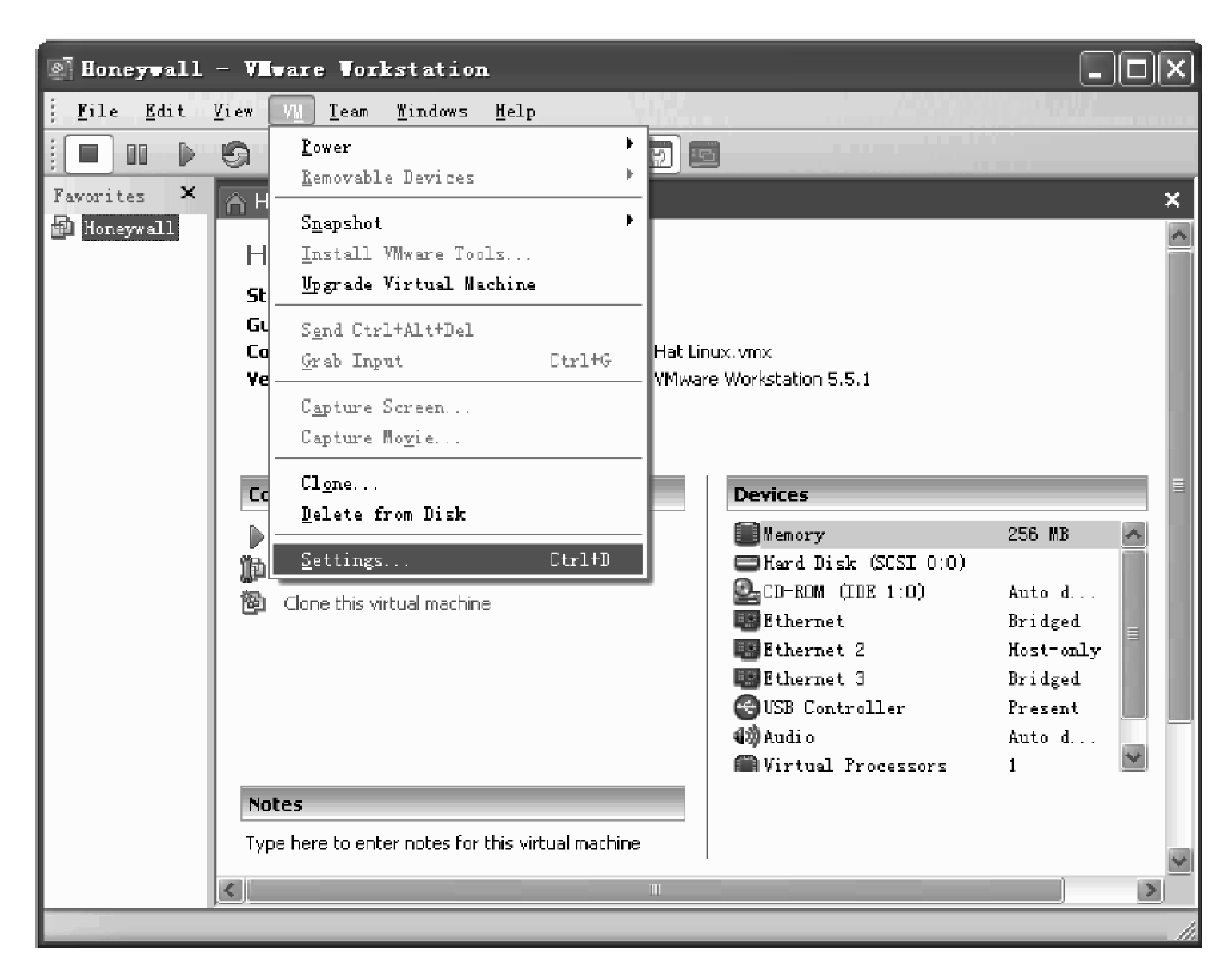


图 8.18　选择设置功能

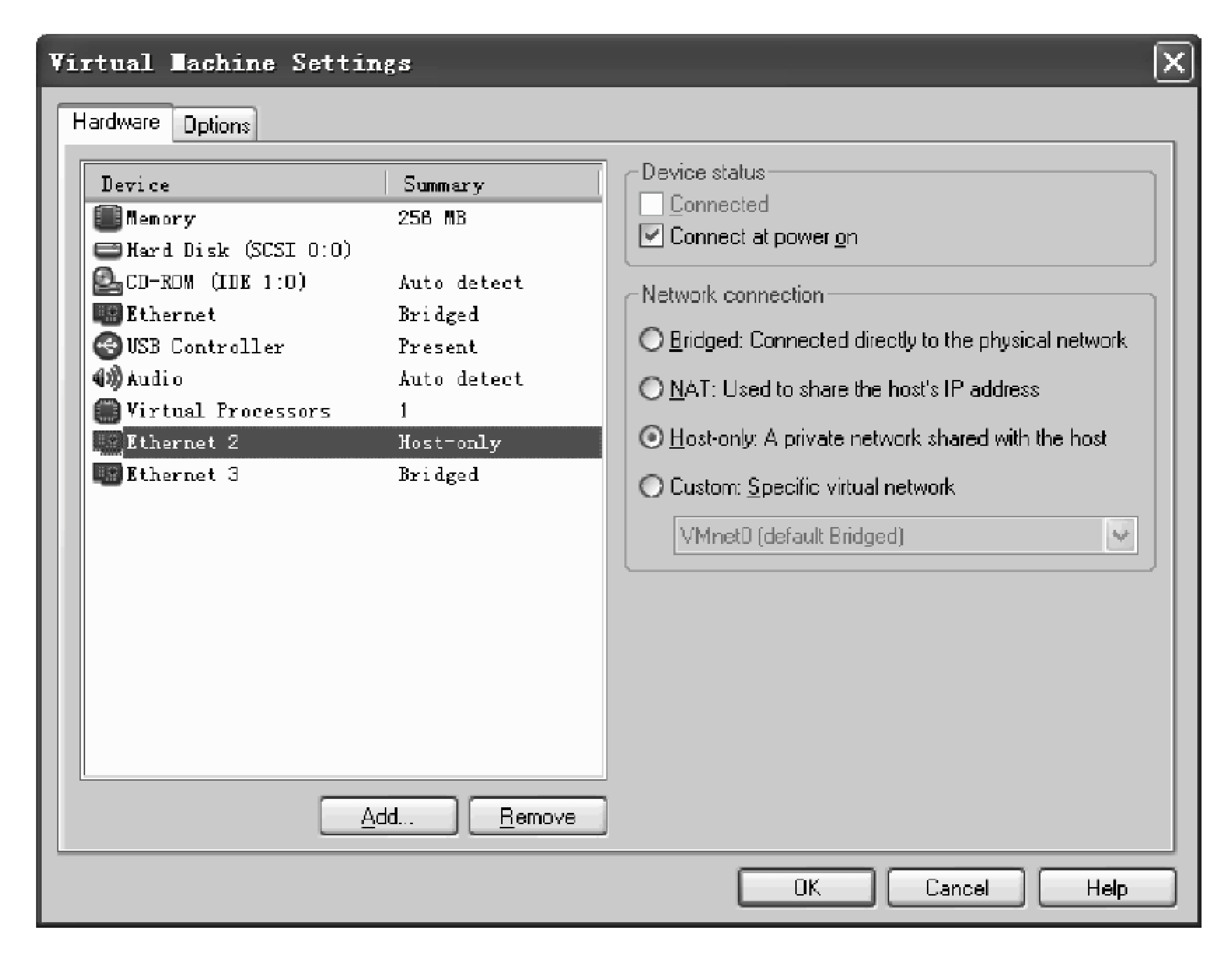


图 8.19　添加网卡

设置 CD-ROM 为蜜网网关，ISO 为 roo v1.0-hw189 软件，如图 8.20 所示。

启动蜜网网关虚拟机，安装蜜网网关软件，按回车键开始安装，如图 8.21 至图 8.23 所示。

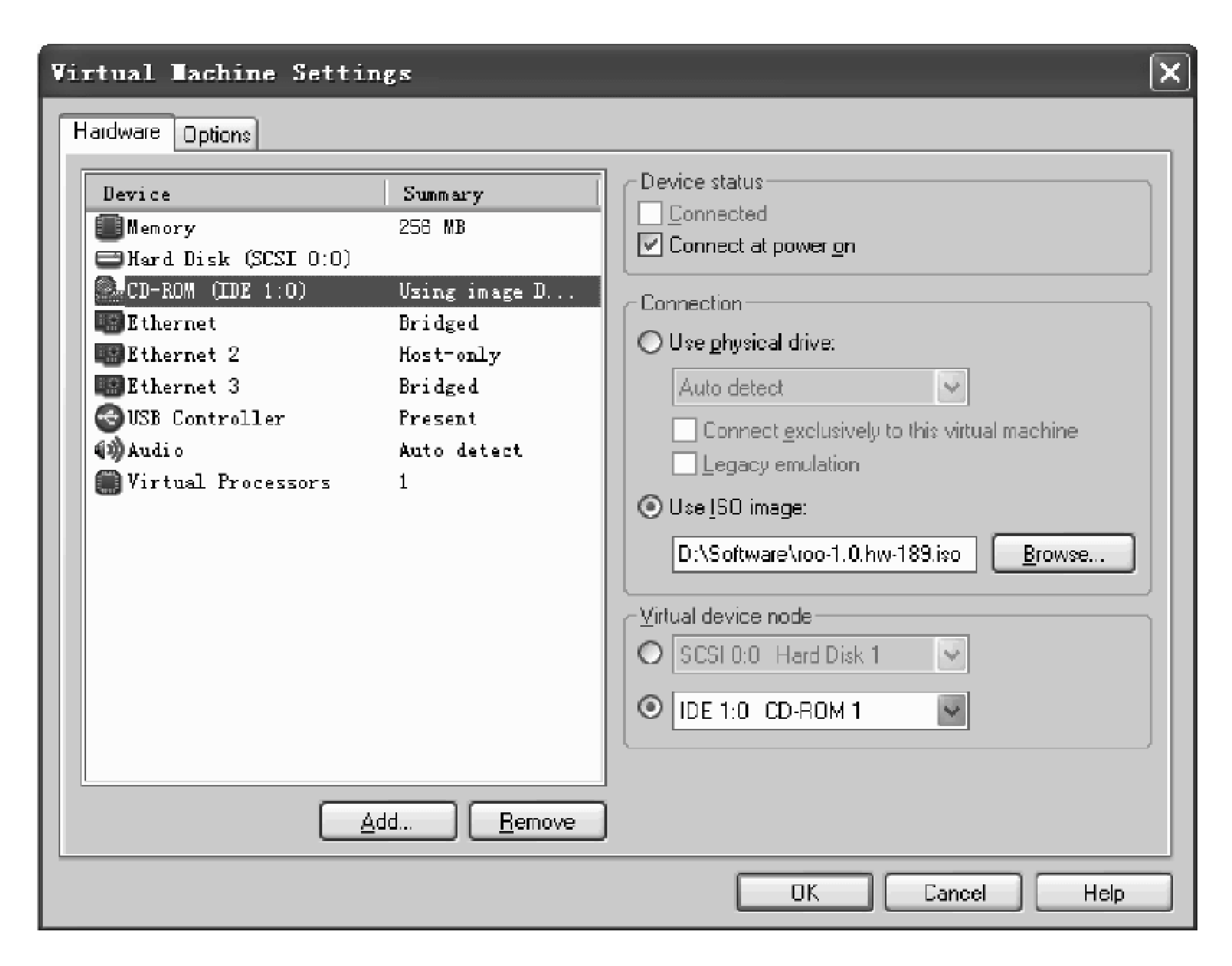


图 8.20 设置 CD-ROM 界面



图 8.21 网关软件安装界面

(3) 配置蜜网网关虚拟机。

以 roo/honey 作为默认用户名/口令登录，使用 su-提升到 root 账号，默认口令也为 honey，如图 8.24 所示。

接下来进行蜜网网关初始配置，如图 8.25 所示。如未能成功进入，则在 shell 中执行第 4 项 Honeywall Configuration 进行设置，如图 8.26 所示。

对 The Honeynet Project 的不承担风险声明选择 Yes，如图 8.27 所示。

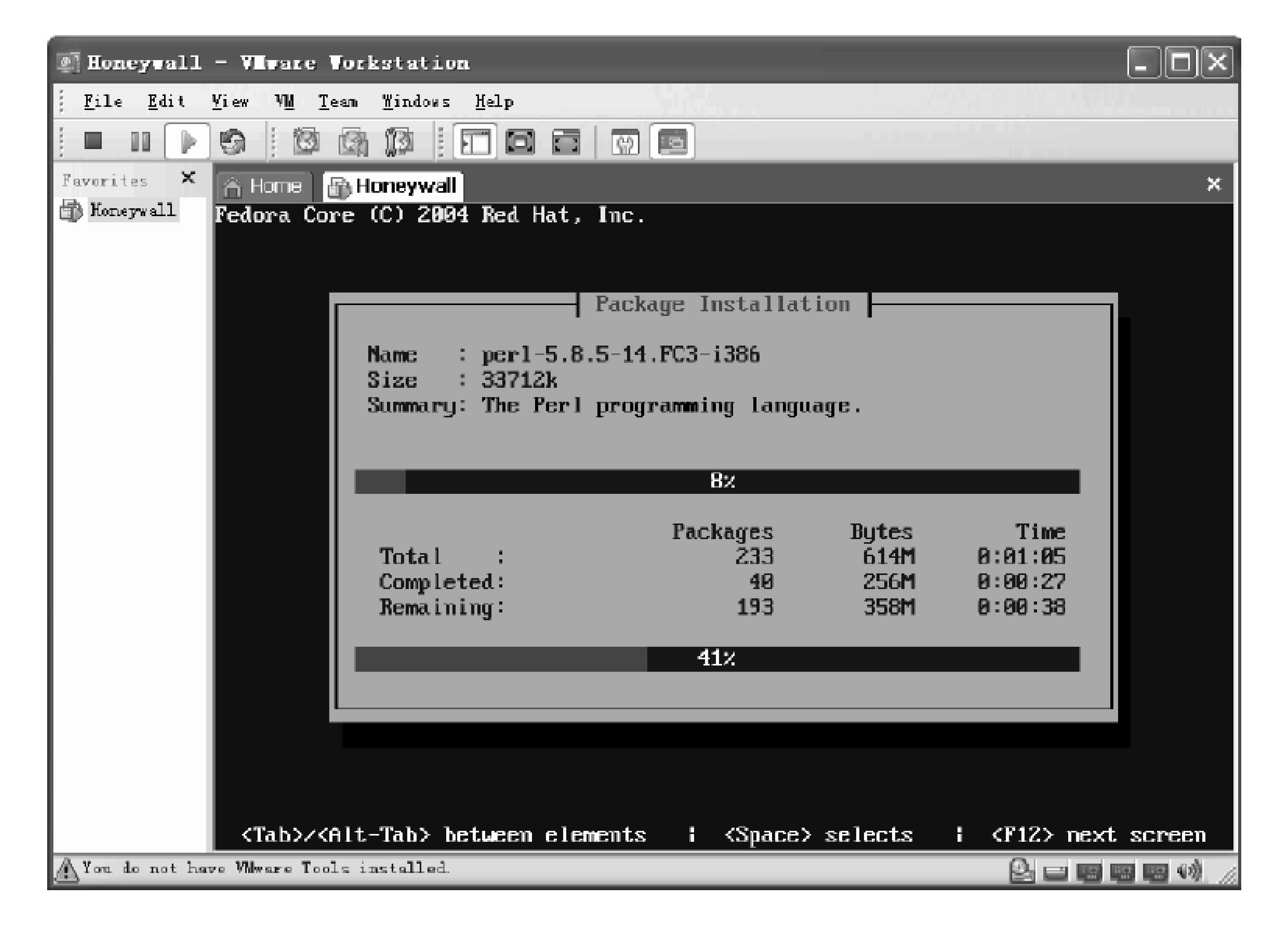


图 8.22 蜜网网关软件安装过程

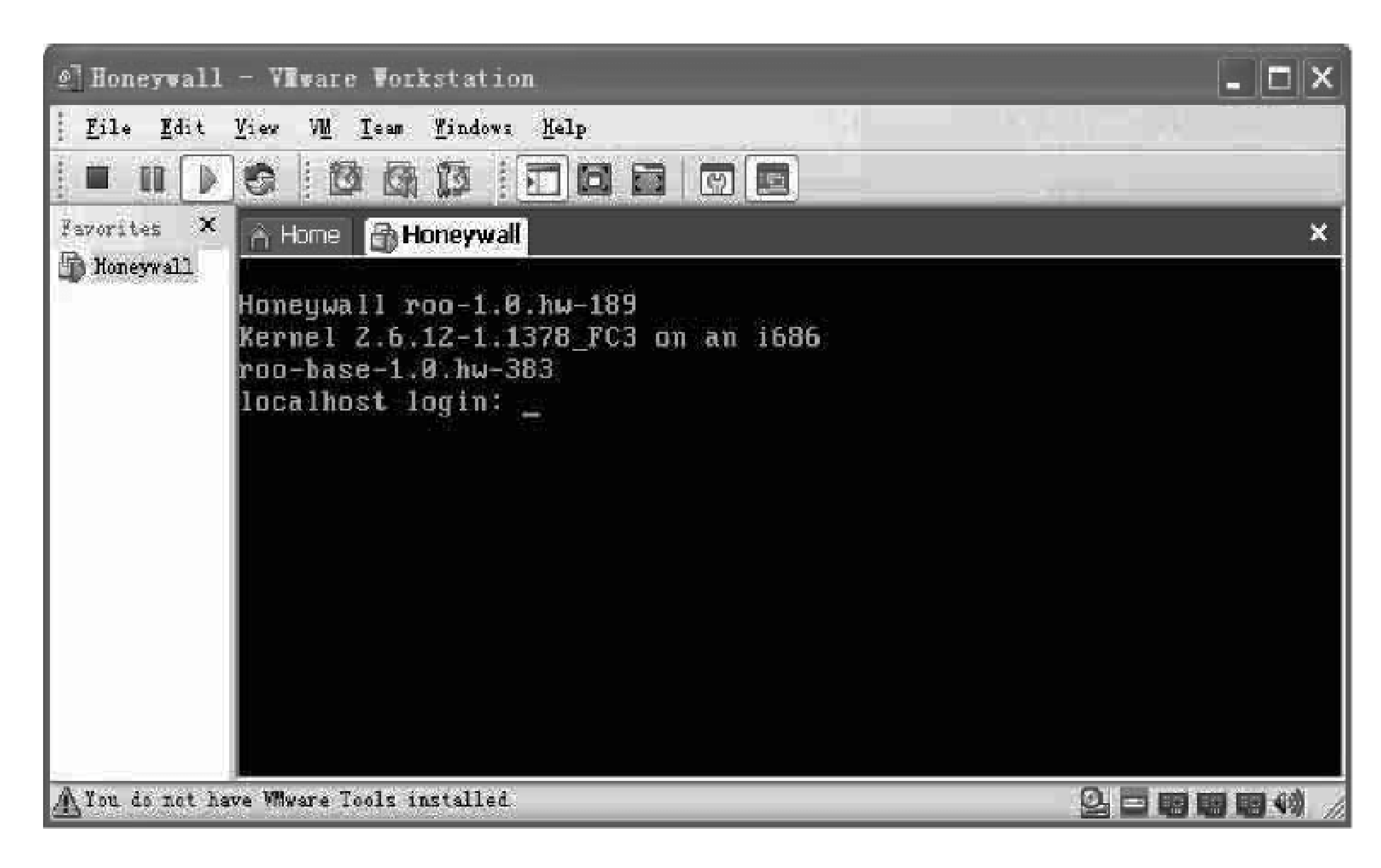


图 8.23 蜜网网关软件安装完毕，进入登录界面

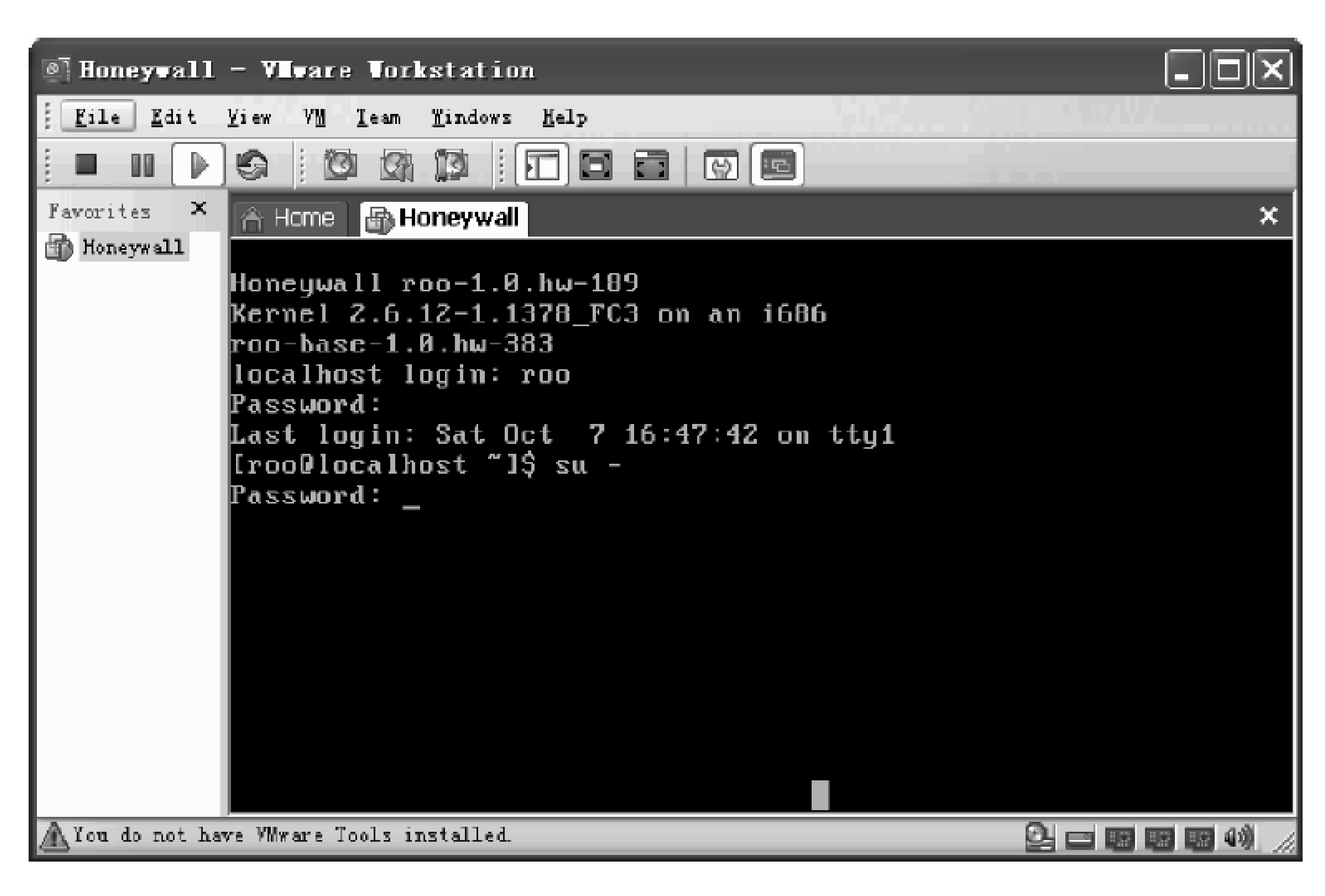


图 8.24 网关登录界面

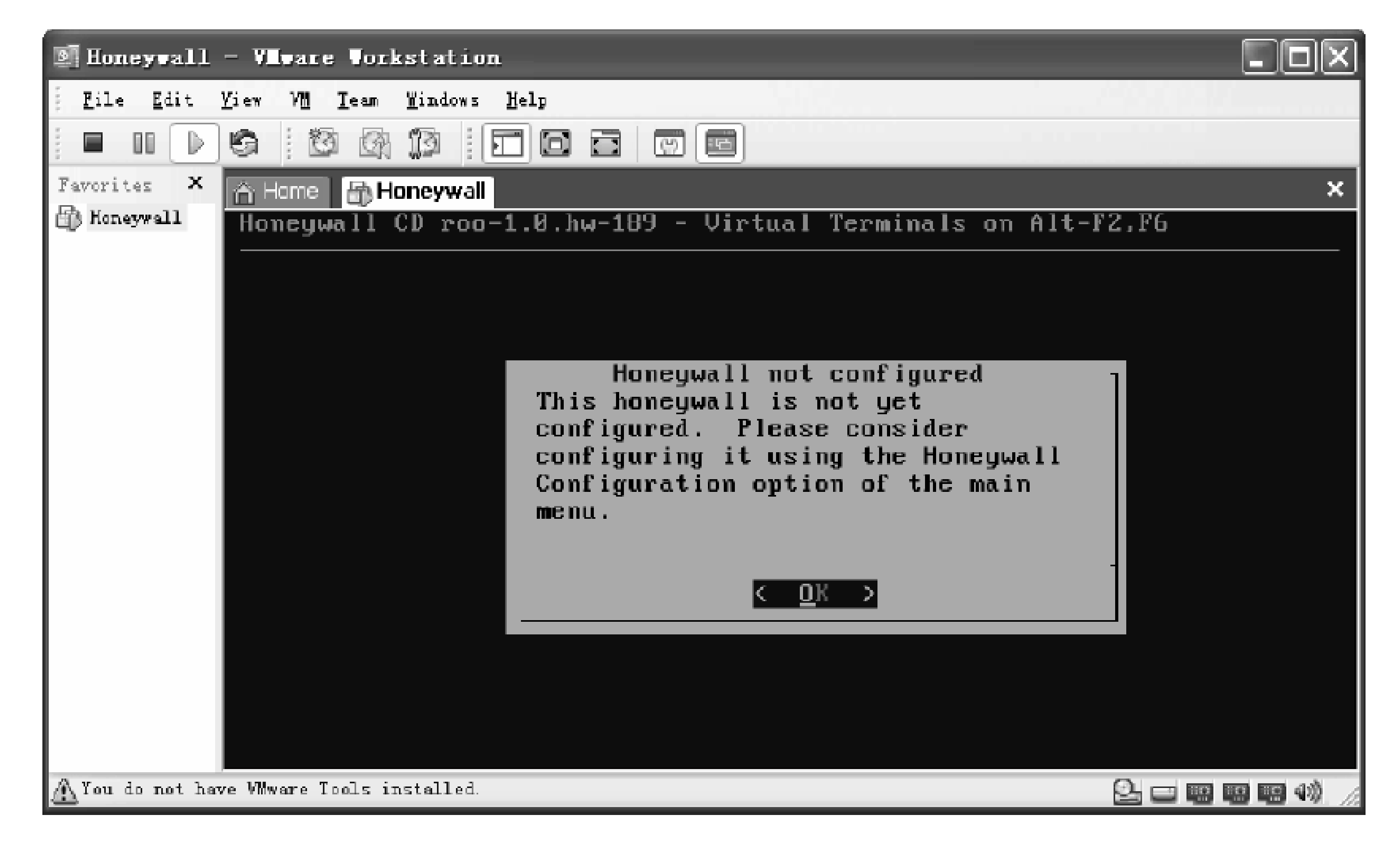


图 8.25 初始设置界面

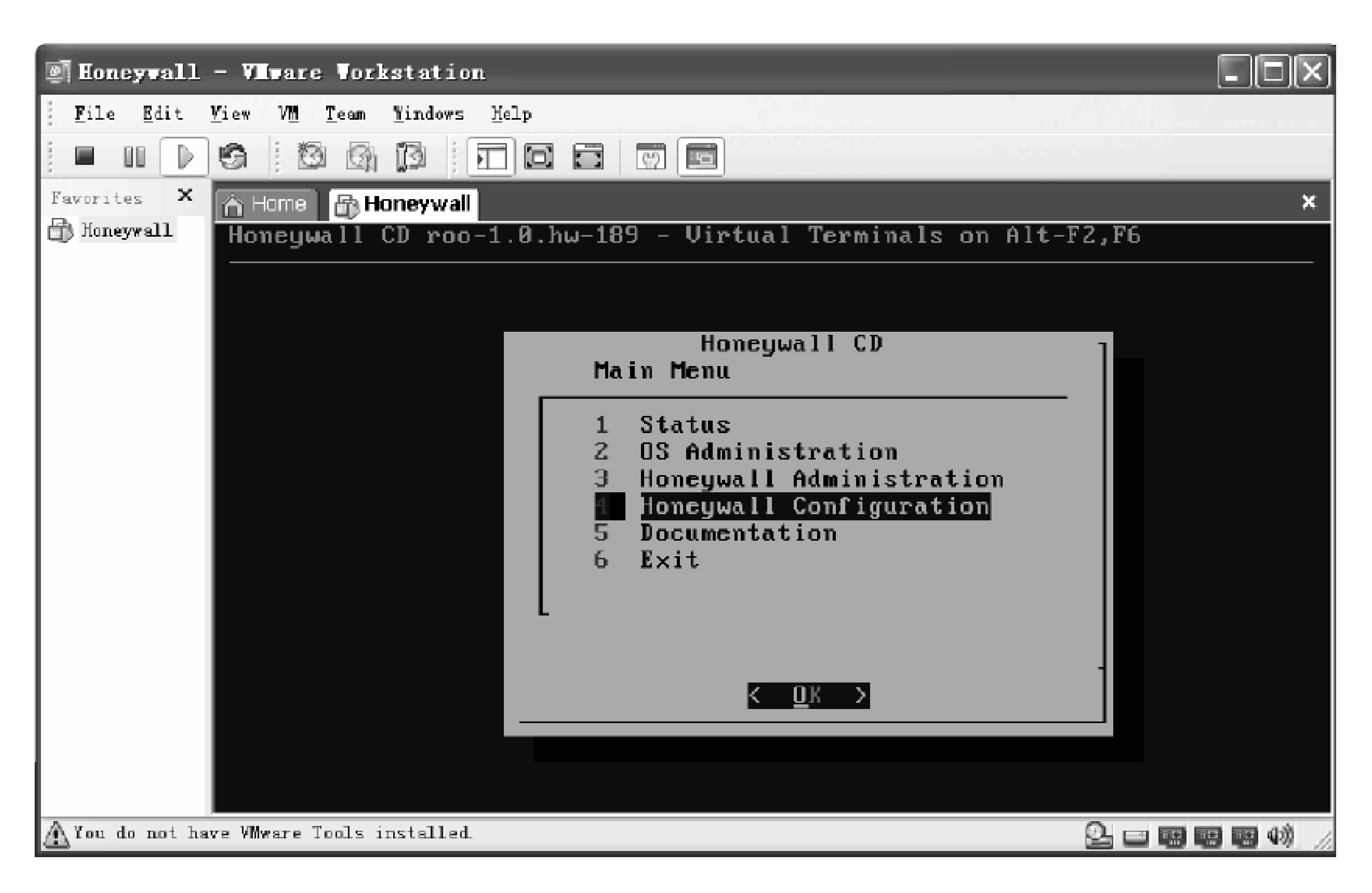


图 8.26 配置菜单选择界面

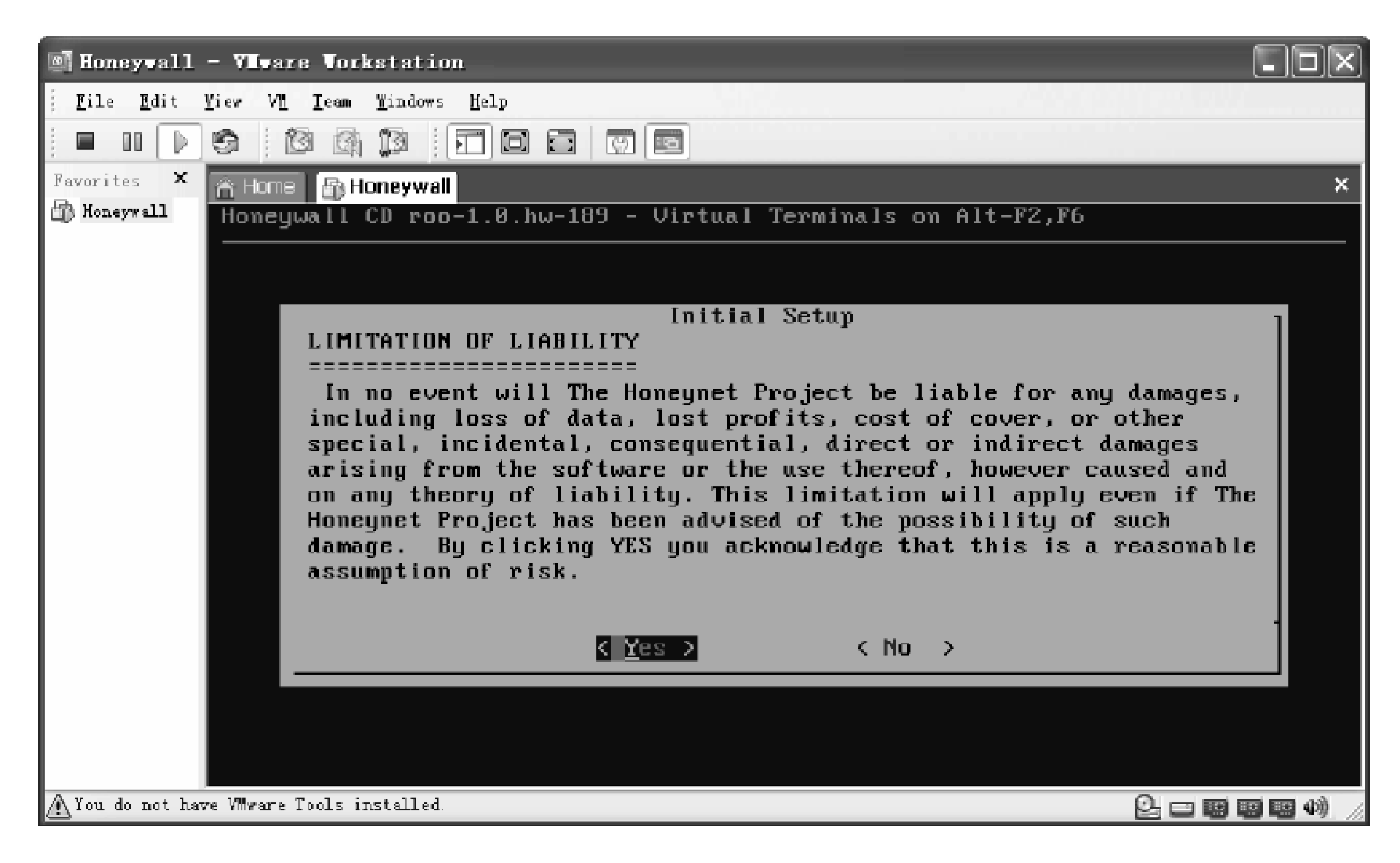


图 8.27 风险声明界面

接下来进行蜜罐信息配置：通过命令行 menu 进入蜜网网关配置界面，选择 4 Honeywall Configuration、1 Mode and IP Information、2 Honeypot IP Address，如图 8.28 所示。通过添加空格来分隔多个 IP 地址，目前 Roo 不支持网络中具有不同网段的蜜罐 IP 地址。

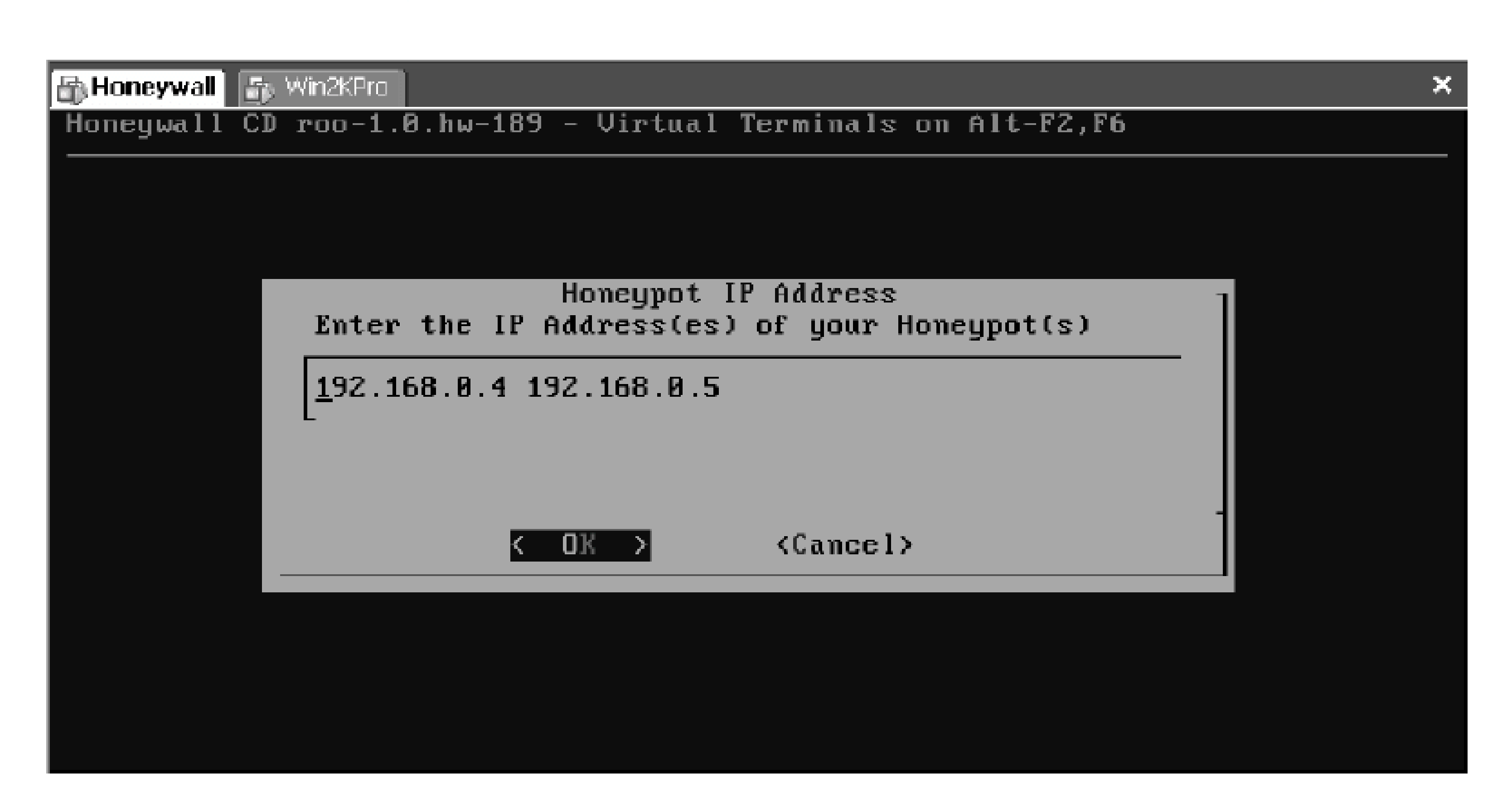


图 8.28　IP 地址设置界面

然后，选择 5 LAN Broadcast Address，设置该网段的广播 IP 地址，如图 8.29 所示。



图 8.29　网段广播 IP 地址设置界面

选择 6 LAN CIDR Prefix，设置为 CIDR 格式，如图 8.30 所示。



图 8.30　蜜网网段设置界面

蜜网网关管理配置：进入蜜网网关配置主界面，选择 4 Honeywall Configuration、2 RemoteManagement、1 Management IP Address，如图 8.31 所示。



图 8.31　管理口 IP地址设置界面

选择 2 Management Netmask，设置 IP 地址掩码，如图 8.32 所示。



图 8.32　管理口 IP地址掩码设置界面

选择 3 Management Gateway，设置管理口网关，如图 8.33 所示。



图 8.33　管理口网关地址设置界面

选择 6 Management DNS Servers，设置 DNS 服务器地址，如图 8.34 所示。



图 8.34 管理口 DNS 服务器地址设置界面

选择 7 Manager，设置可以管理蜜网网关的远程控制端 IP 范围，以 CIDR 格式填写，可有多个 IP 网段，中间用空格分隔，如图 8.35 所示。



图 8.35 被管理网段设置界面

Sebek 服务器端配置：在蜜网网关配置主界面中，选择 4 Honeywall Configuration、11 Sebek，Sebek 服务器端 IP 地址设置为管理口 IP，目标端口选择为 1101，Sebek 数据包处理选择为 Drop，如图 8.36 所示。



图 8.36 Sebek 服务器端 IP 地址设置界面

(4) 测试蜜网网关的远程管理。

首先,使用 SecureCRT 软件测试 SSH 远程管理,远程 SSH 连接蜜网网关管理口,如图 8.37 所示。

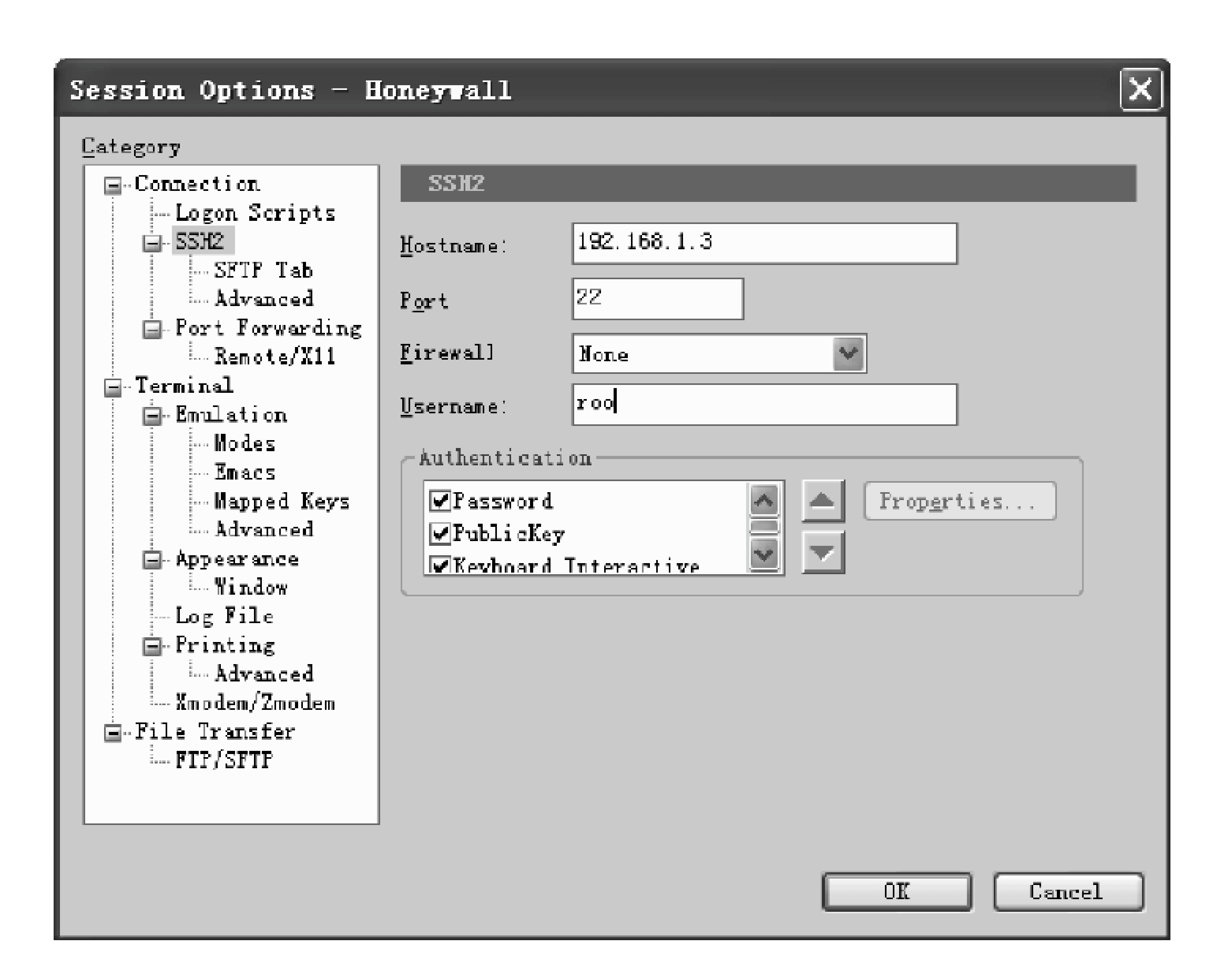


图 8.37　SSH 远程管理设置界面

其次,测试 Walleye 远程访问情况,如图 8.38、图 8.39 所示。

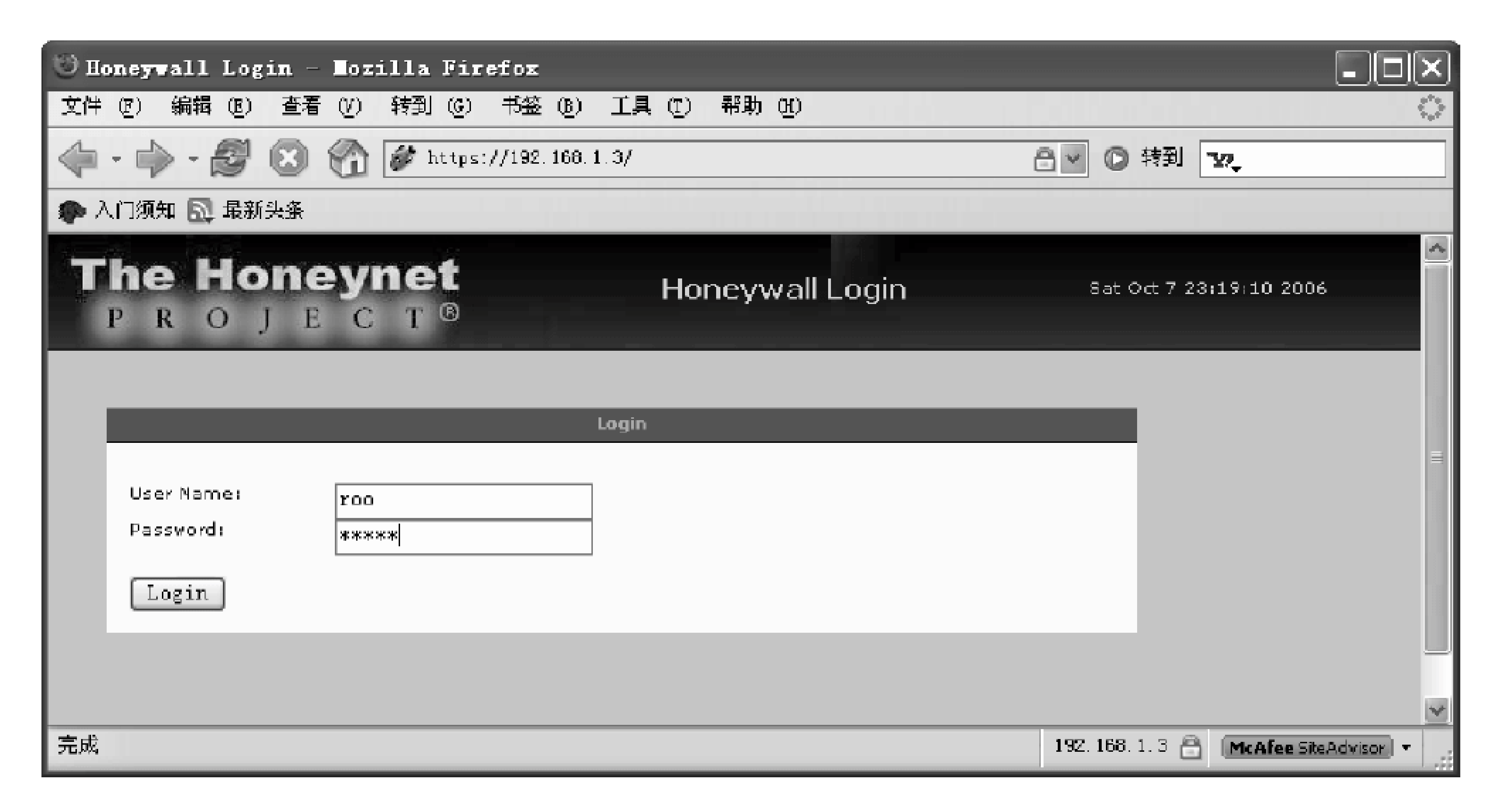


图 8.38　远程连接 Walleye 界面

(5) 安装虚拟机蜜罐。

首先,新建虚拟机,配置虚拟硬件,如图 8.40 所示。

配置虚拟机蜜罐的网络接口,如图 8.41 所示。

测试虚拟机蜜罐和宿主主机之间的网络连接,在宿主主机上 ping 虚拟机蜜罐 IP,如图 8.42 所示为宿主主机到虚拟机的连通测试。

在虚拟机蜜罐上 ping 宿主主机 IP,如图 8.43 所示为虚拟机到宿主主机的连通测试。

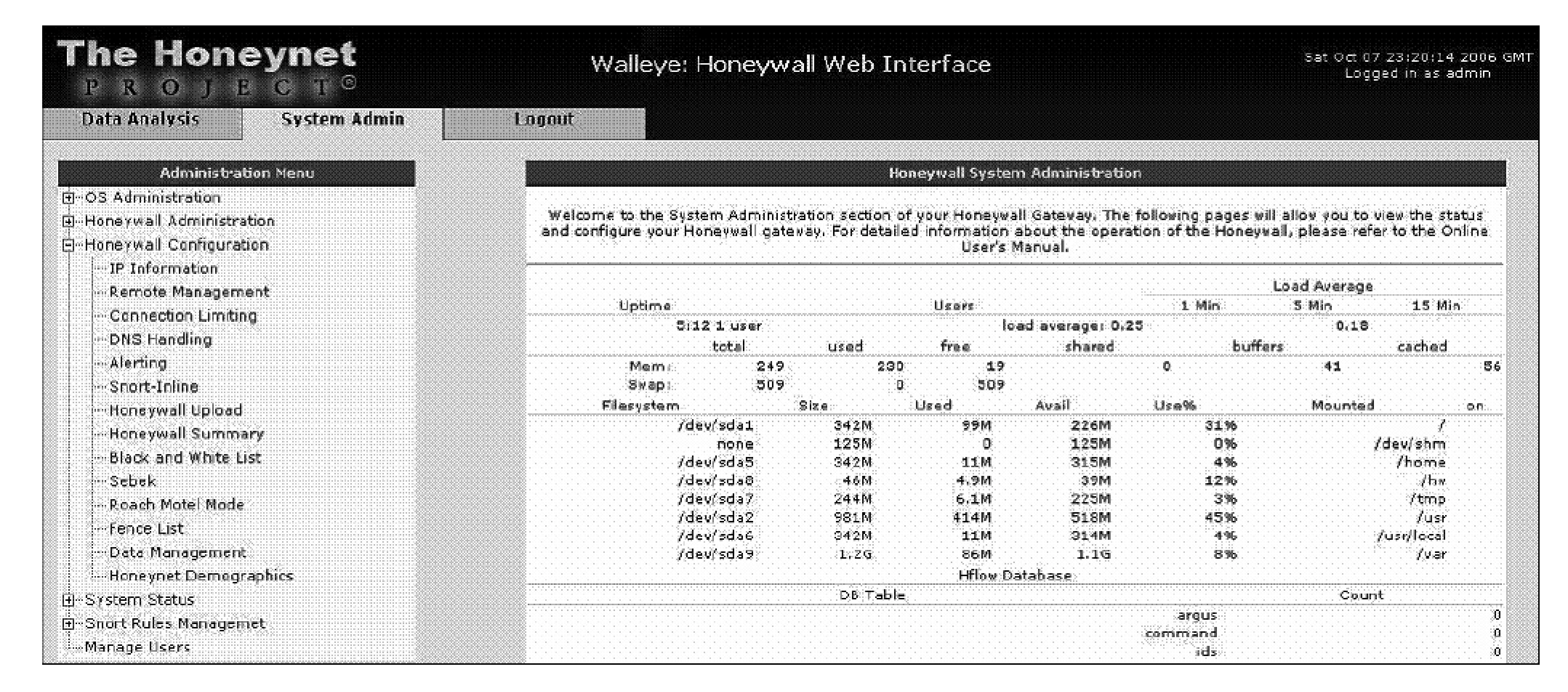


图 8.39　Walleye 远程管理界面

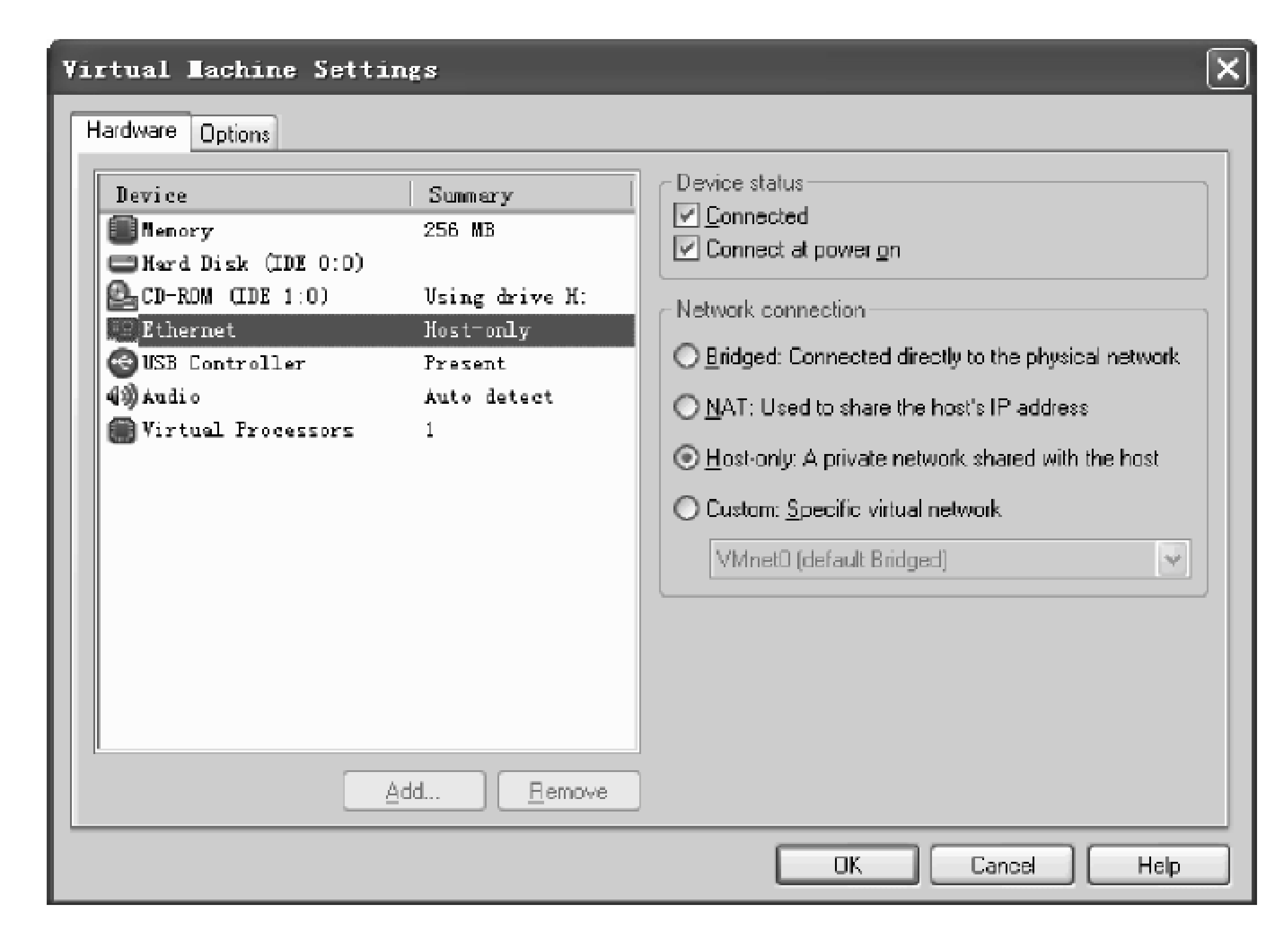


图 8.40　虚拟硬件设置界面

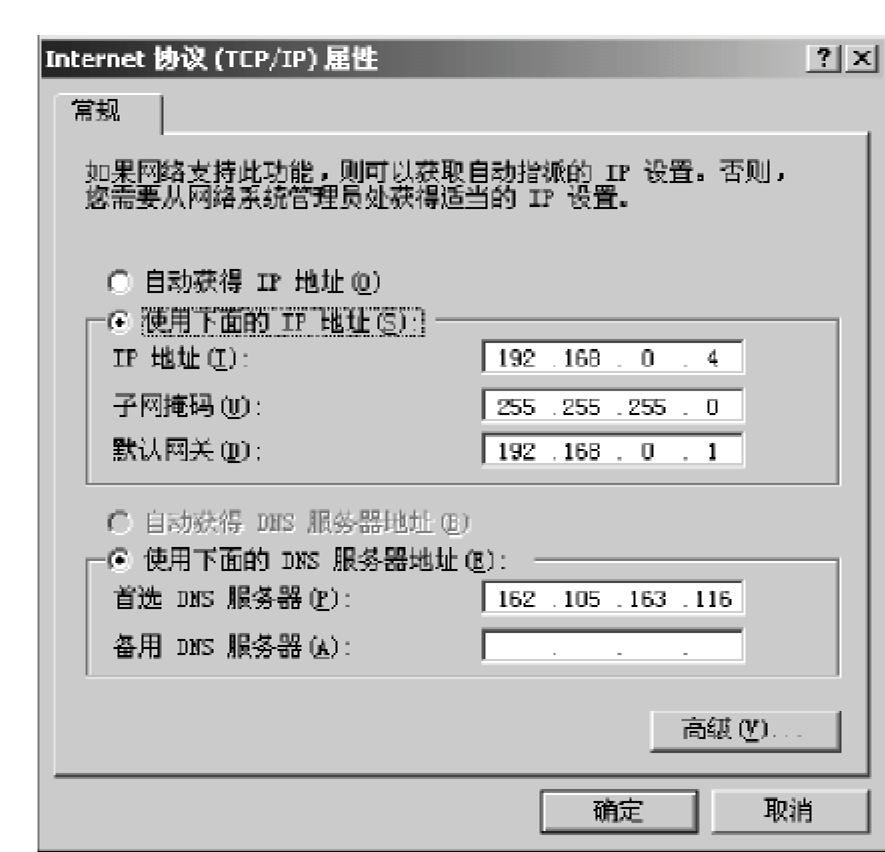


图 8.41　虚拟蜜罐 IP 地址设置界面

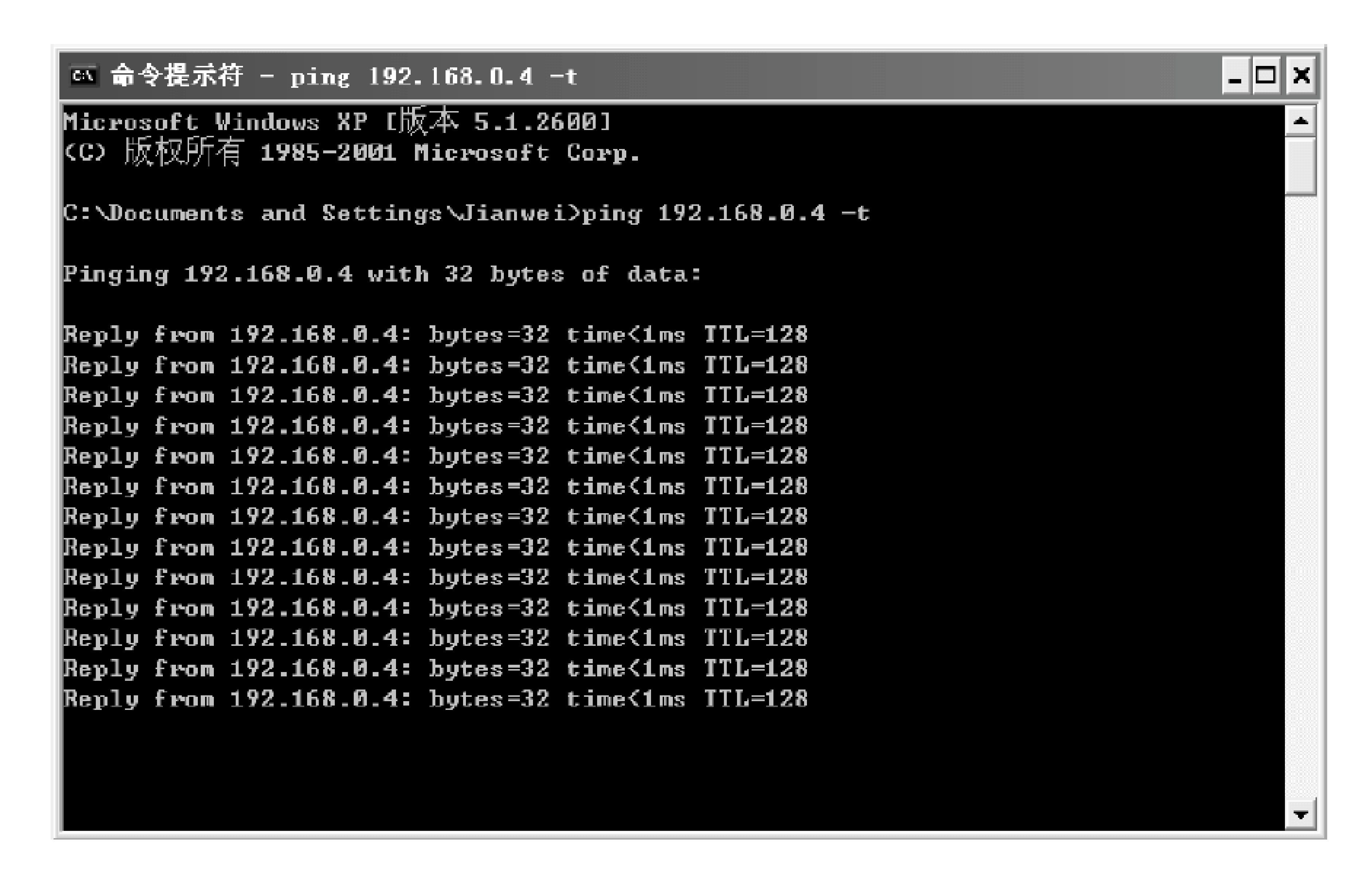


图 8.42　宿主主机到虚拟机的连通测试

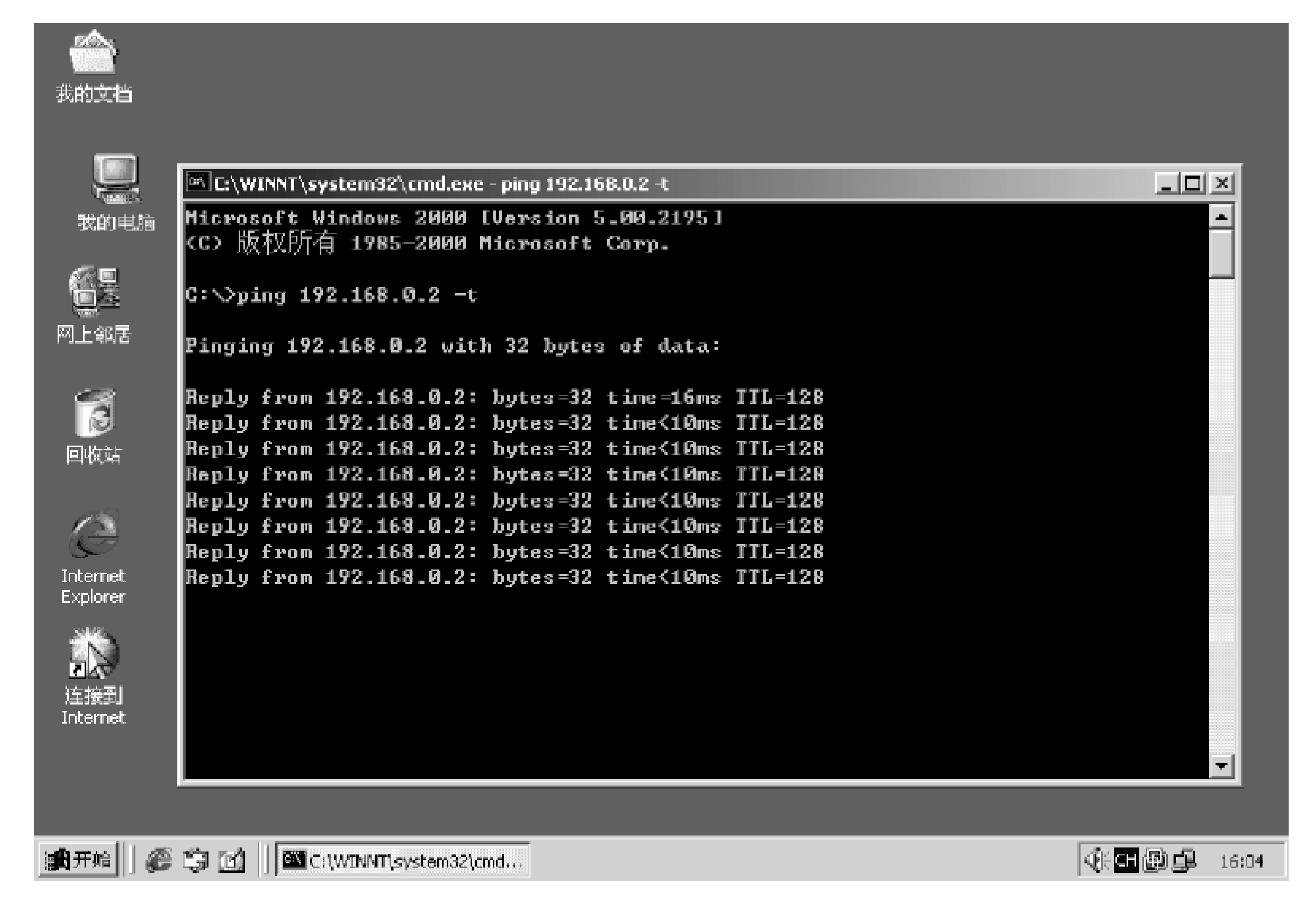


图 8.43　虚拟机到宿主主机的连通测试

在蜜网网关上监听 ICMP ping 包是否通过外网口和内网口：

```
tcpdump -i eth0 icmp
tcpdump -i eth1 icmp
```

通过测试后，说明虚拟机蜜罐和外部网络之间的网络连接没有问题。

(6) 在虚拟机蜜罐上安装 Sebek 客户端。

将 Sebek-Win32-3.0.4.zip(http://www.savidtech.com/sebek/)通过网络共享复制到虚拟机蜜罐中，解压后执行 Setup.exe 进行安装。

在蜜网网关虚拟机上执行 ifconfig eth2，得到管理口 eth2 的 MAC 地址，填入如图 8.44 所示的 Sebek 服务器端配置对话框。

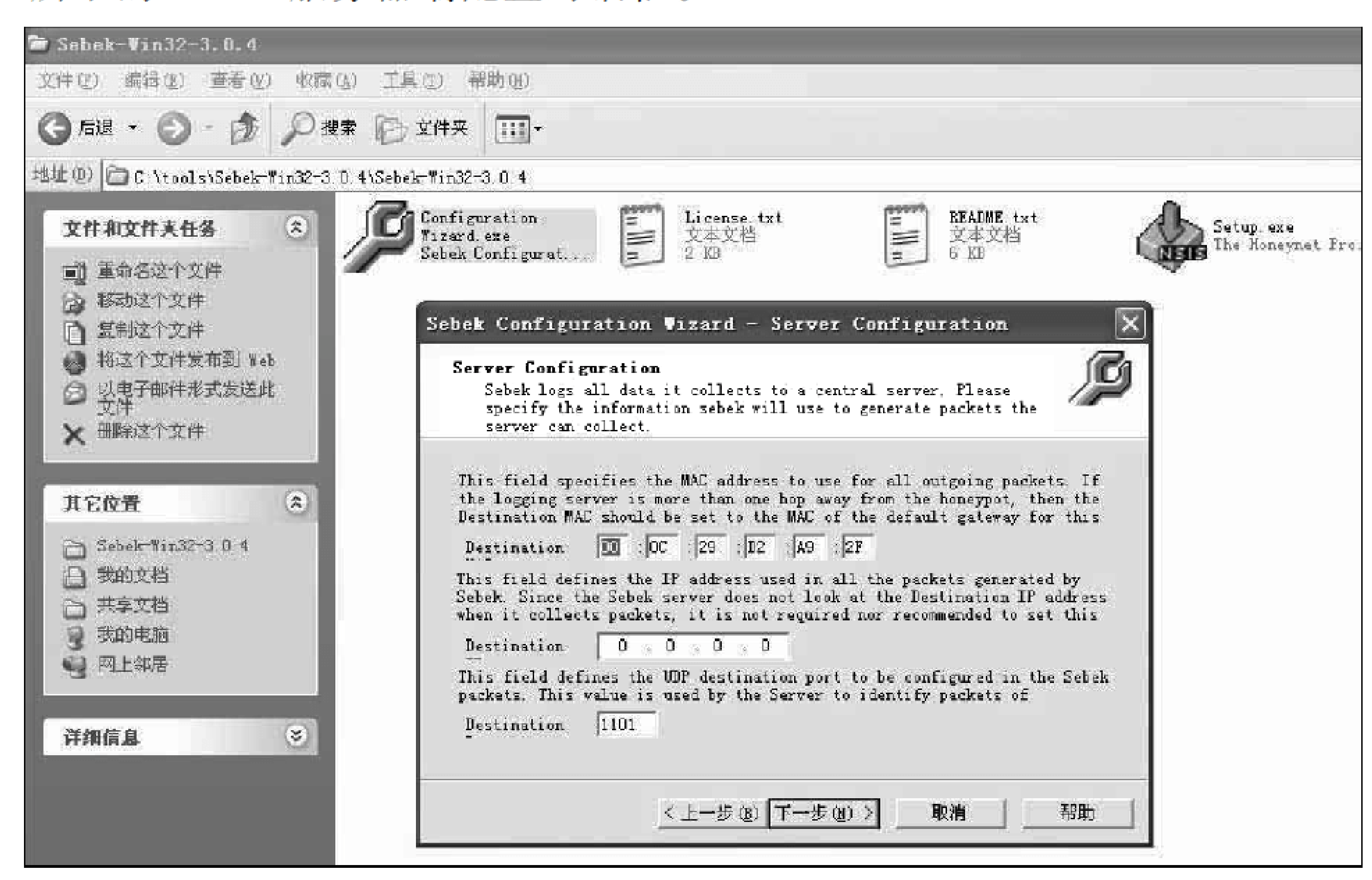


图 8.44　监控软件设置界面

随机生成或填写 Magic Number，需保证同一蜜网中每台蜜罐主机上均安装 Sebek，且 Sebek 使用的 Magic Number 保持一致，使得 Sebek 的上传通信在蜜网中对攻击者隐蔽(即使攻击者获取了蜜罐主机的控制权，并启用网络监听器进行监听)。重新启动主机，建立 Snapshot。至此，整个虚拟蜜网搭建环节全部结束。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

8.3 漏洞扫描实验

实验器材

- 蜜网综合环境 1 套。
- PC(Windows XP/Windows 7)1 台。

预习要求

- 做好实验预习，复习虚拟蜜网技术的有关内容。
- 熟悉虚拟蜜网的使用方法。
- 熟悉实验过程和基本操作流程。
- 做好预习报告。

实验任务

掌握利用虚拟蜜网技术进行系统漏洞扫描的方法。

实验环境

操作系统为 Windows XP 的 PC 一台。

预备知识

- 蜜网技术。
- 虚拟蜜网原理。

实验步骤

(1) 在攻击机(即宿主主机)上运行 XScan 漏洞扫描工具对 192.168.0.4 虚拟机蜜罐实施漏洞扫描，如图 8.45 所示。

(2) 在蜜网网关上对 XScan 漏洞扫描过程中的每个网络连接都进行了完备的记录，从如图 8.46 所示的蜜网网关数据摘要视图可发现正在扫描的 192.168.0.2 攻击机 IP，图 8.47 则显示了其扫描的每个网络连接详细信息。

实验报告要求

- 实验目的。

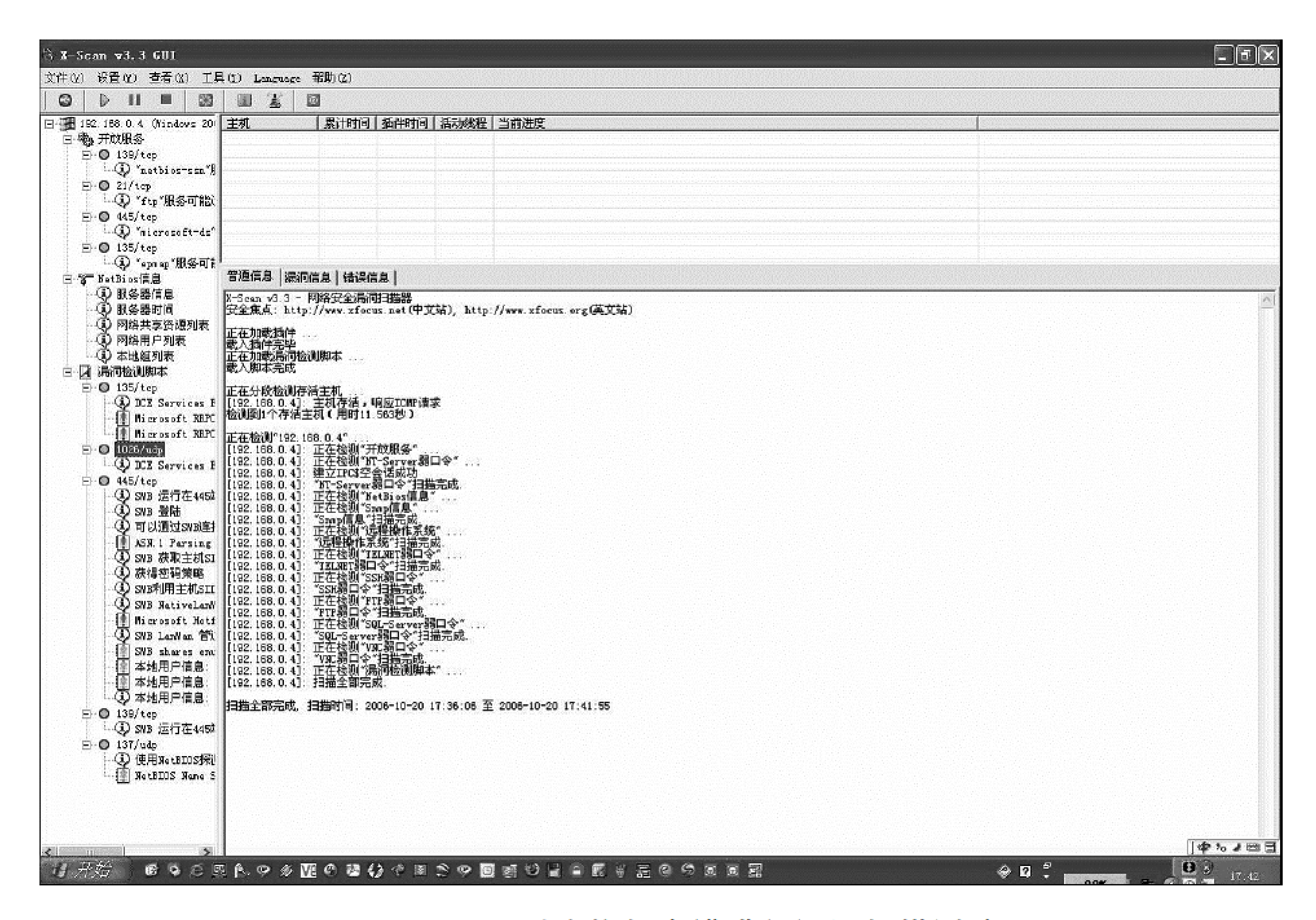


图 8.45　XScan 对虚拟机蜜罐进行漏洞扫描测试

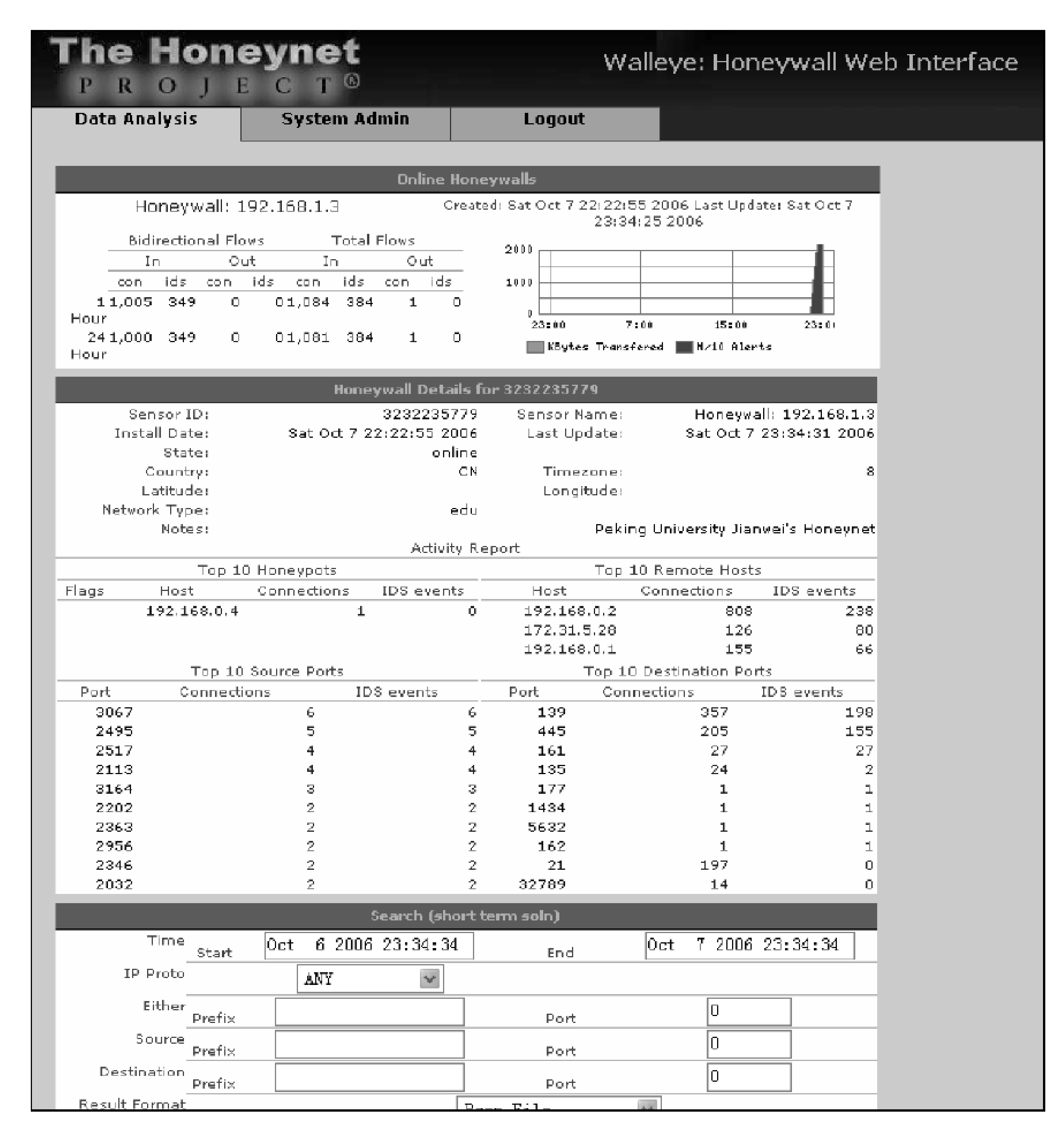


图 8.46　蜜网网关捕获的漏洞扫描过程的摘要视图

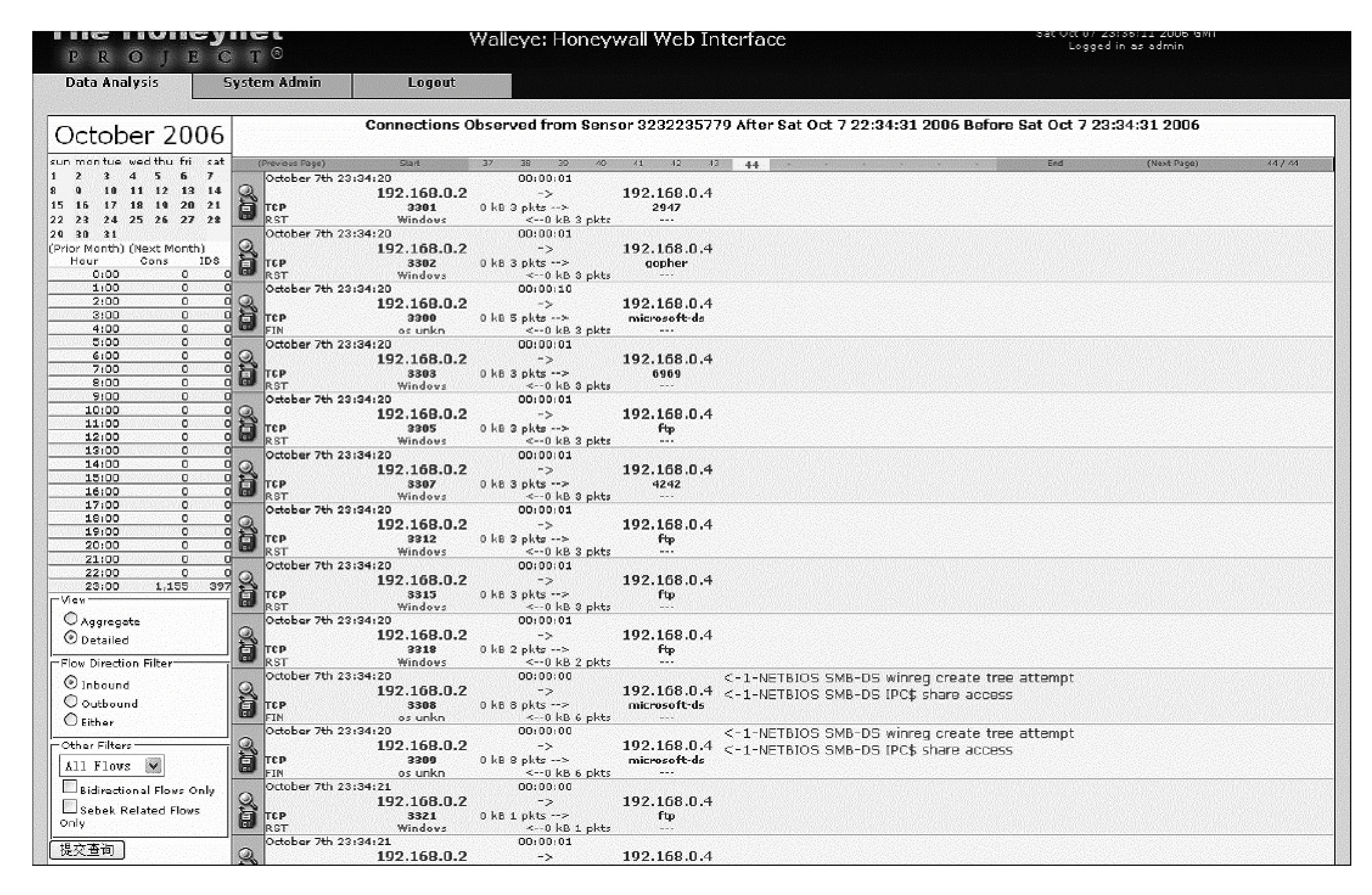


图 8.47　扫描网络连接视图

- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

8.4　渗透攻击实验

实验器材

- 虚拟蜜网软件综合系统 1 套。
- PC(Windows XP/Windows 7)1 台。

预习要求

- 做好实验预习,复习虚拟蜜网技术的有关内容。
- 熟悉虚拟蜜网的使用方法。
- 熟悉实验过程和基本操作流程。
- 做好预习报告。

实验任务

掌握利用虚拟蜜网技术进行系统渗透攻击扫描的方法。

实验环境

操作系统为 Windows XP 的 PC 一台。

预备知识

- 蜜网技术。
- 虚拟蜜网原理。

实验步骤

（1）在宿主主机上安装 Metasploit 渗透攻击工具：从 http://www.metasploit.com/projects/Framework/downloads.html 下载 Metasploit Framework 2.6 for Windows 并安装。

（2）Metasploit 渗透攻击测试：运行 MSFConsole，输入针对 MS05-039 即插即用服务漏洞的渗透攻击命令，获得反向的 Shell，如图 8.48 所示。（注：需打开宿主主机的个人防火墙，如微软防火墙，使得能够接收 4444 端口的连入。）

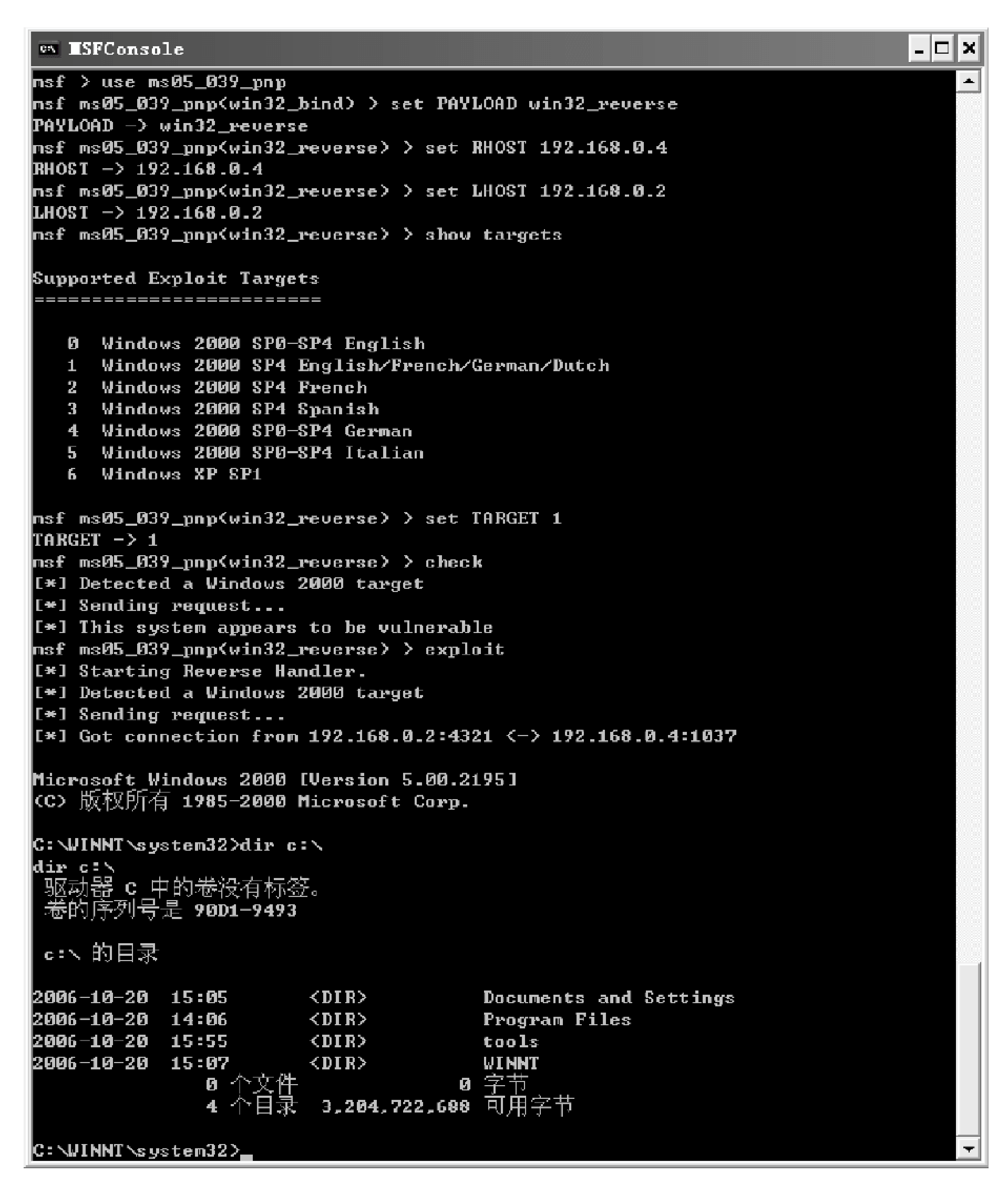


图 8.48　MS05-039漏洞渗透攻击过程

（3）对蜜网网关记录的攻击数据进行分析，验证蜜网的攻击数据捕获和分析功能，如图 8.49 至图 8.54 所示。

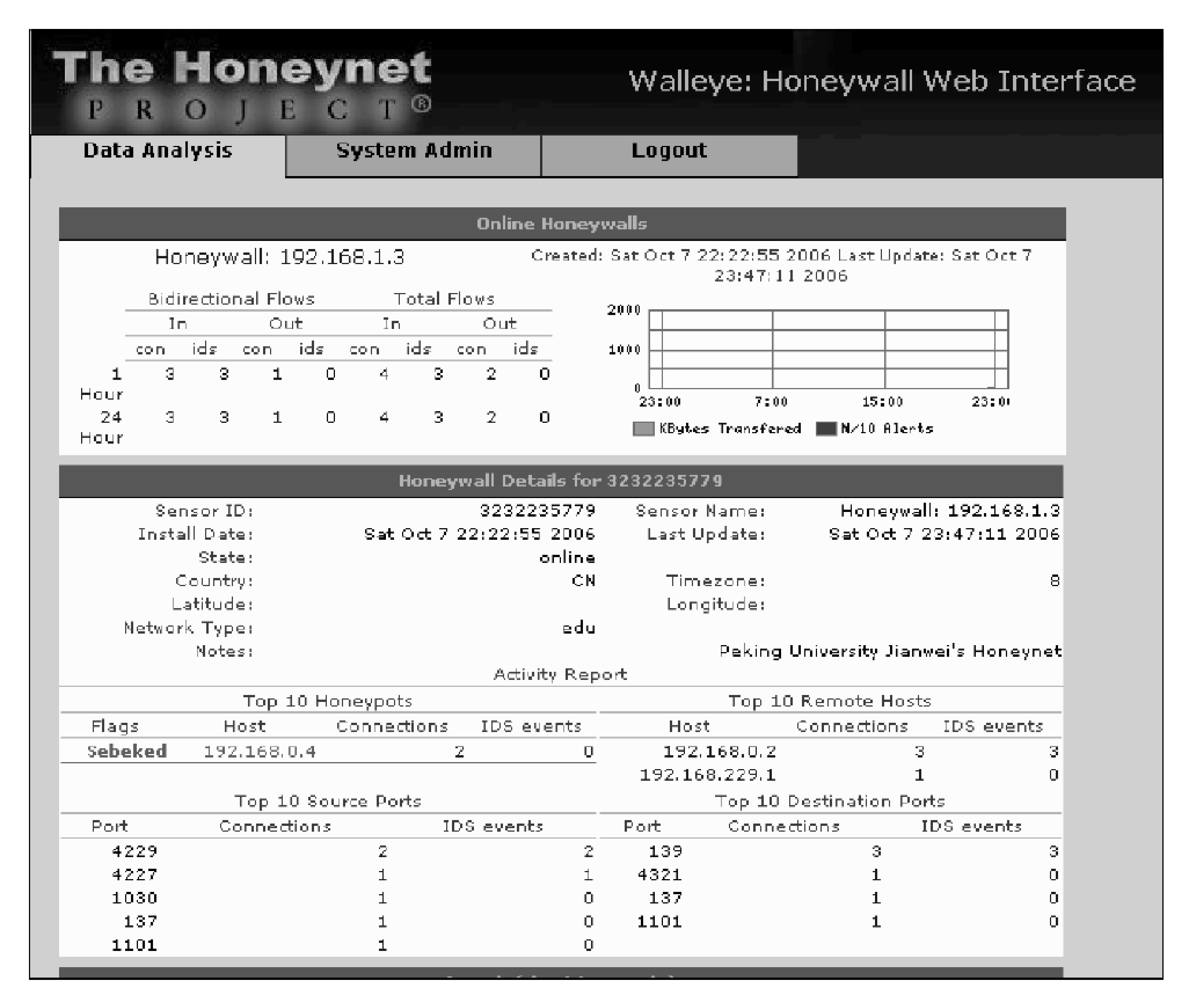


图 8.49　蜜网网关对渗透攻击测试的摘要视图

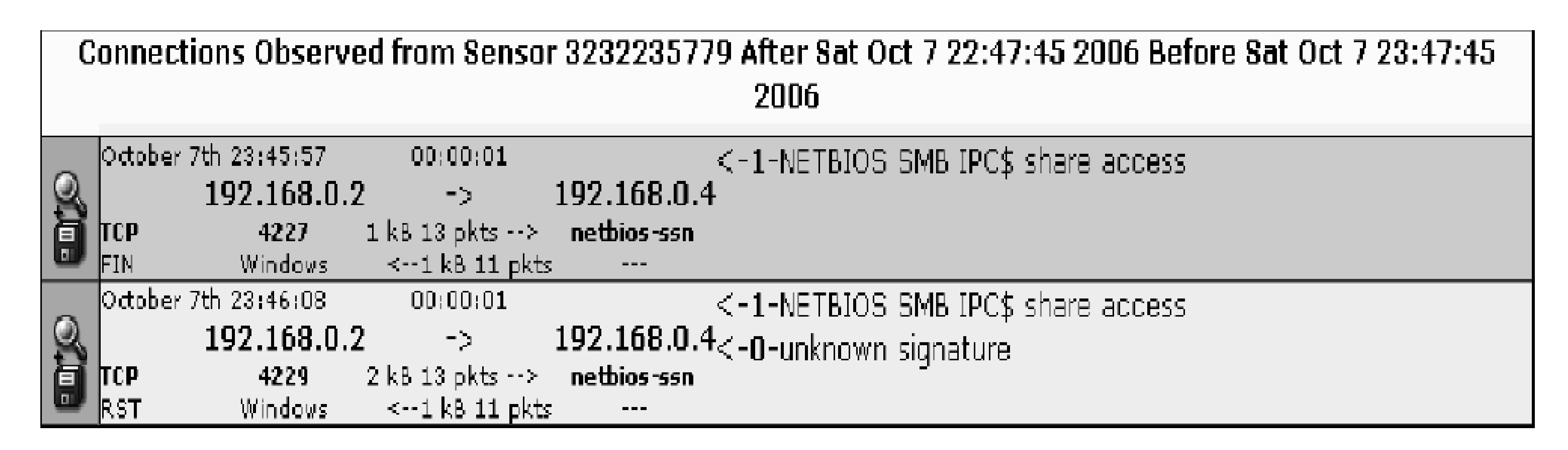


图 8.50　向蜜罐主机发起的向内连接视图（对应 check 和 exploit）

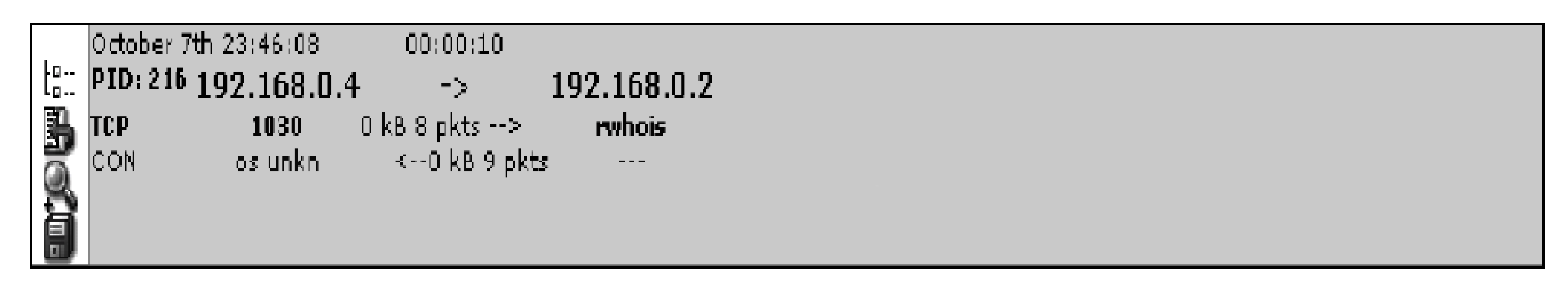


图 8.51　向外发起的反向 Shell 连接

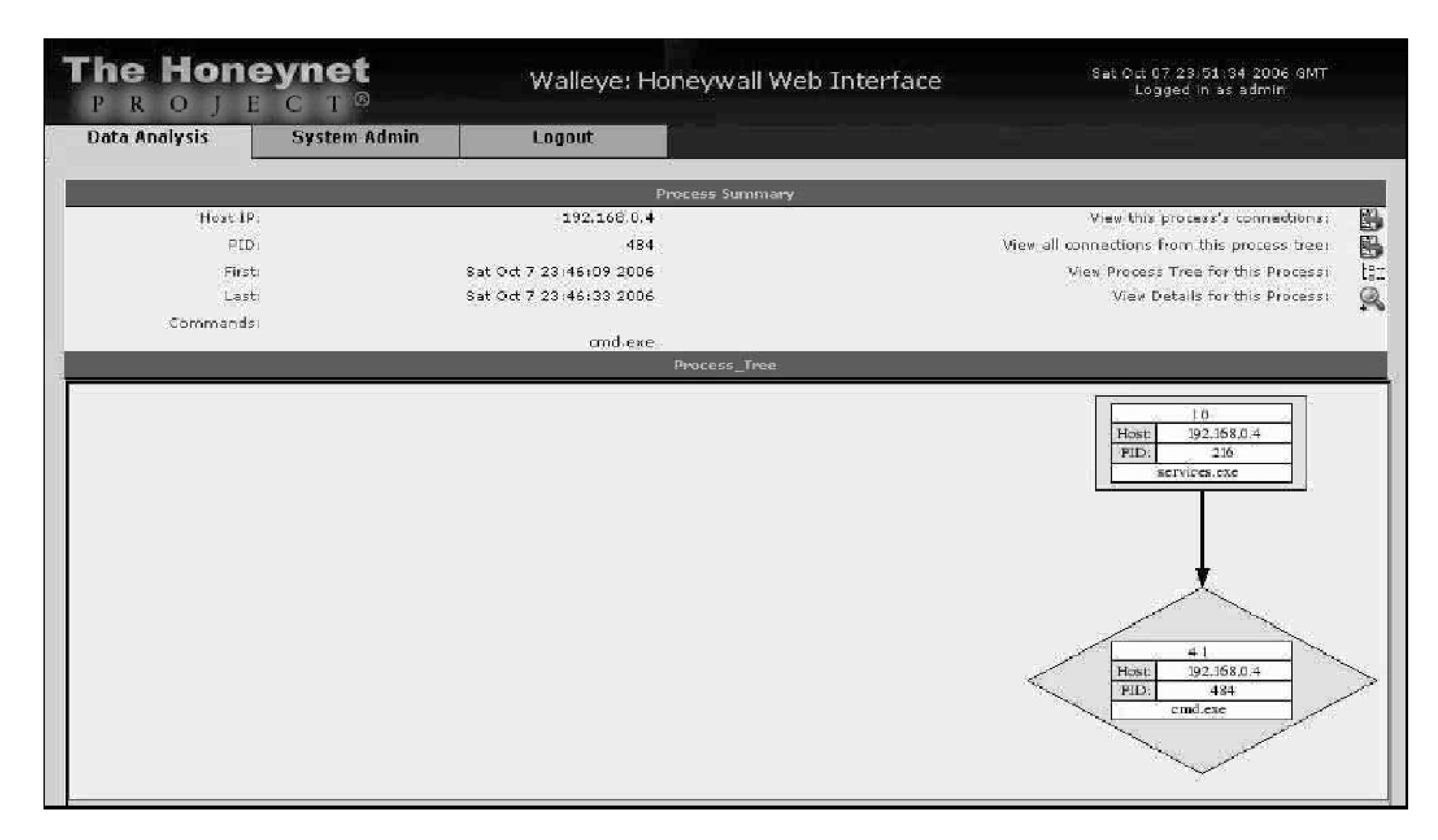


图 8.52　反向 Shell 连接对应的详细进程视图

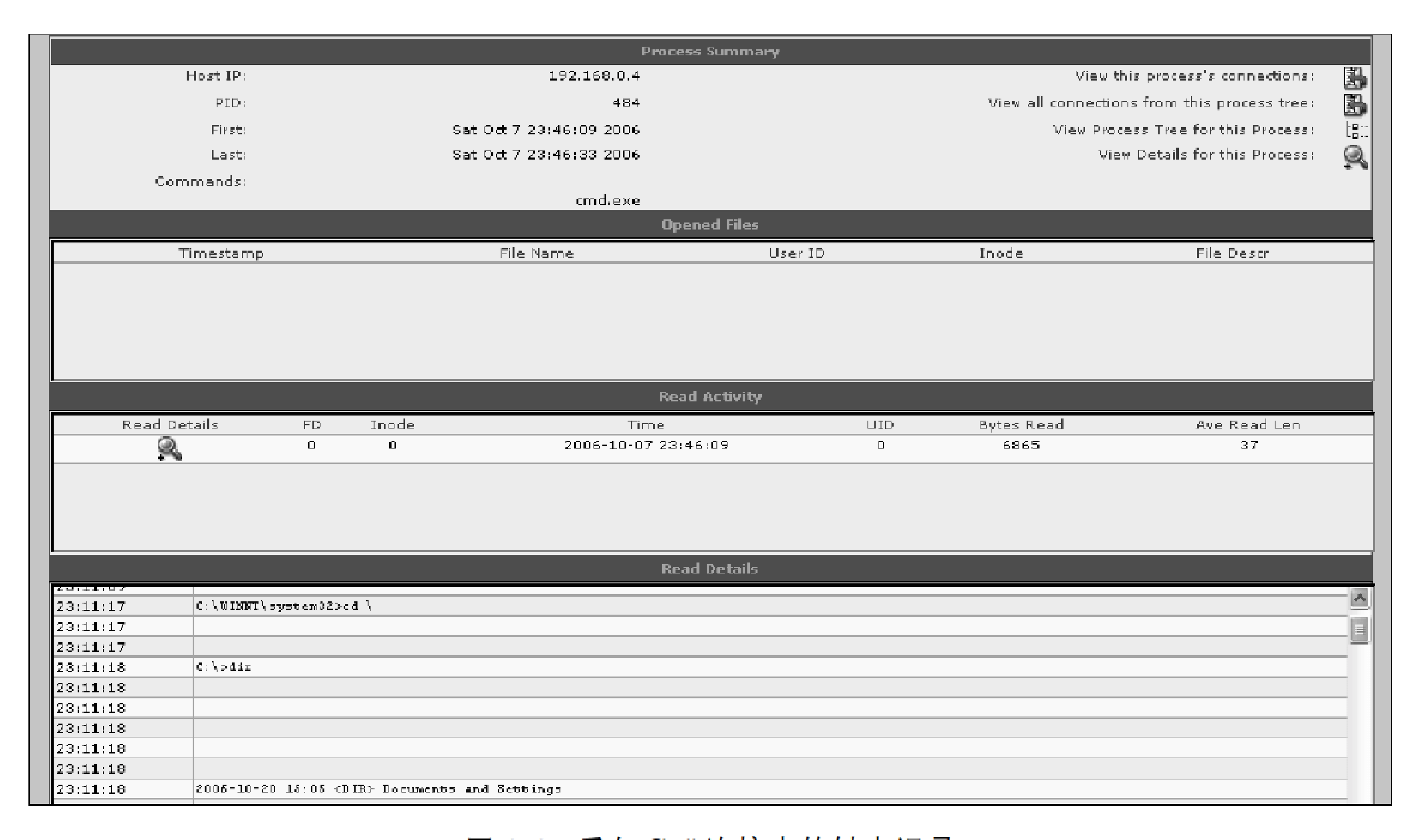


图 8.53　反向 Shell 连接中的键击记录

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

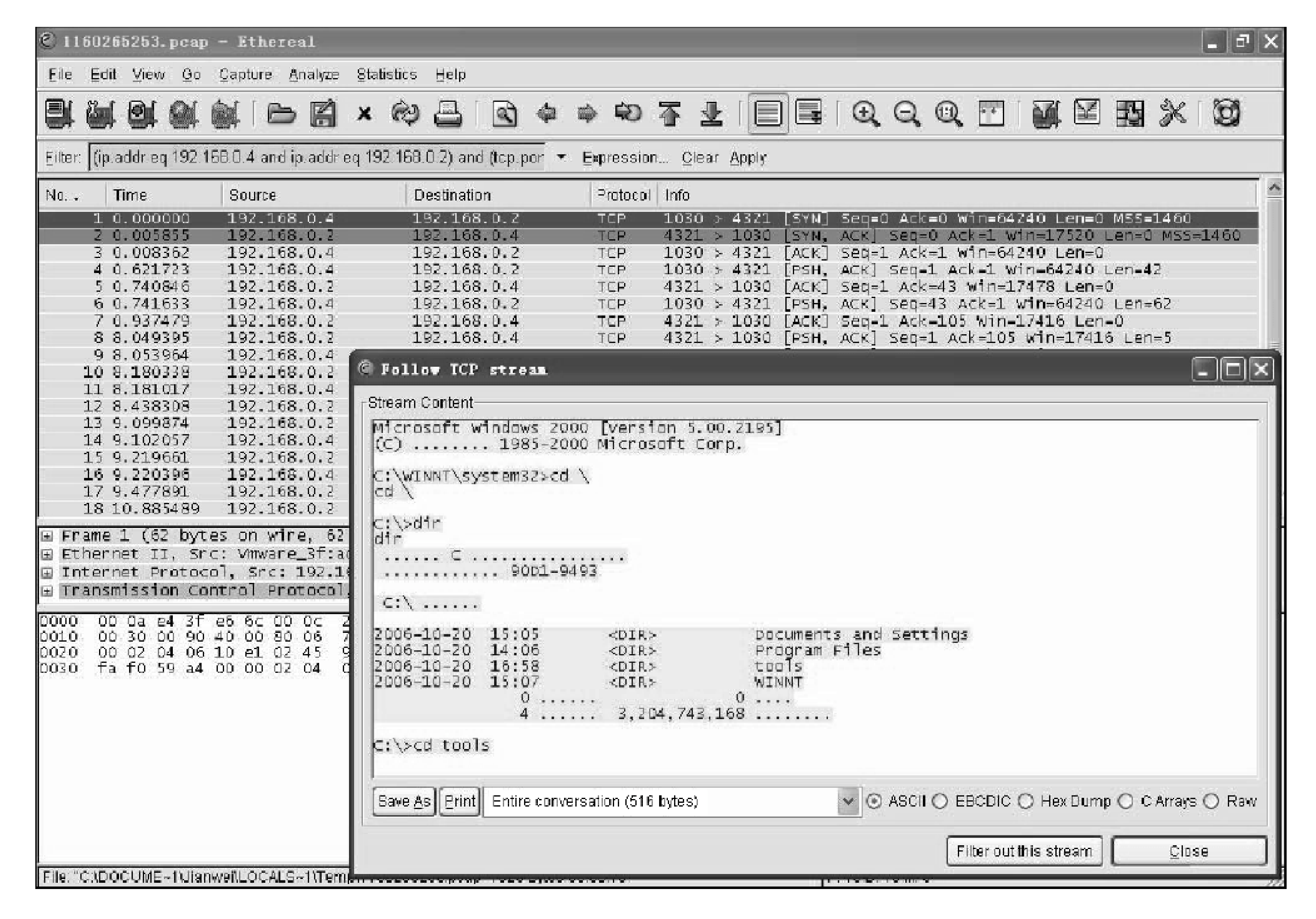


图 8.54 反向 Shell 连接原始数据包流重组结果

参考文献

[1] 陆璐,刘发贵. 基于 Web 的远程监控系统. 北京：清华大学出版社,2008.

[2] (美)麦克卢尔,等,著.黑客大曝光.钟向群,郑林,译.北京：清华大学出版社，2010.

[3] (美)西蒙斯基,等,著.Sniffer Pro 网络优化与故障检修手册. 陈逸,等,译. 北京：电子工业出版社，2004.

[4] 张同光,等.信息安全技术使用教程. 北京：电子工业出版社，2008.

[5] (美)科瑞奥,著.Snort 入侵检测实用解决方案. 吴溥峰,等,译. 北京：机械工业出版社，2005.

[6] 唐正军，李建华. 入侵检测技术. 北京：清华大学出版社，2004.

[7] 熊华,郭世泽,吕慧勤. 网络安全：取证与蜜罐. 北京：人民邮电出版社，2003.

[8] 吴秀梅. 防火墙技术及应用教程. 北京：清华大学出版社，2010.